ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

GROUPS OF MOTIONS AND RICCI DIRECTIONS

BY LUTHER PFAHLER EISENHART

(Received June 21, 1935)

1. In order that a Riemannian space V_n with the fundamental form

$$g_{ij}dx^i dx^j \tag{1.1}$$

admit a group G_1 of motions, whose equations are

$$x'^i = f^i(x; a), \tag{1.2}$$

it is necessary and sufficient that the following equations be satisfied

$$g_{ij}(x) = g_{kl}(x') \frac{\partial x'^k}{\partial x^i} \frac{\partial x'^l}{\partial x^j}, \tag{1.3}$$

where $g_{kl}(x')$ are the same functions of the x''s as g_{kl} are of the x's.[1] For the infinitesimal transformation of the G_1, namely

$$x'^i = x^i + \xi^i \delta t, \tag{1.4}$$

equations (1.3) are equivalent to the equations of Killing, namely

$$\xi^k \frac{\partial g_{ij}}{\partial x^k} + g_{ih} \frac{\partial \xi^h}{\partial x^j} + g_{jh} \frac{\partial \xi^h}{\partial x^i} = 0. \tag{1.5}$$

We remark that equations (1.3) are of the form holding for tensors but such that the g's on the right are of the same functional form as the corresponding g's on the left; thus the g's are carried into themselves by a motion. The same applies to any tensor whose components are functions of the g's and their derivatives.[2] In particular we have

$$R_{ij}(x) = R_{kl}(x') \frac{\partial x'^k}{\partial x^i} \frac{\partial x'^l}{\partial x^j}, \tag{1.6}$$

where R_{ij} are the components of the Ricci tensor.[3] From (1.4) and (1.6) we have

$$\xi^k \frac{\partial R_{ij}}{\partial x^k} + R_{ih} \frac{\partial \xi^h}{\partial x^j} + R_{jh} \frac{\partial \xi^h}{\partial x^i} = 0. \tag{1.7}$$

---

[1] R. G., p. 233; C. G., p. 216, Ex. 2; these references are to the author's *Riemannian Geometry* and *Continuous Groups of Transformations*, respectively. The summation convention for repeated indices is used throughout this paper,

[2] This observation applies also to other differential invariants; cf., C. G., pp. 229–231.

[3] R. G., p. 21.

We assume that V_n is not an Einstein space, that is $R_{ij} \neq \rho g_{ij}$, and that if the form (1.1) is not positive definite the elementary divisors of the characteristic equation

$$|R_{ij} - \rho g_{ij}| = 0 \tag{1.8}$$

are simple. If the roots of (1.8) are simple, an orthogonal ennuple of unit contravariant vectors of components λ^i_{α}, where α indicates the vector and i the components, is uniquely determined by

$$(R_{ij} - \rho_{\alpha} g_{ij})\lambda^i_{\alpha} = 0, \tag{1.9}$$

where λ^i_{α} correspond to the root ρ_{α}. Thus we have

$$g_{ij}\lambda^i_{\alpha}\lambda^j_{\alpha} = e_{\alpha} \quad (\alpha \text{ not summed}), \qquad g_{ij}\lambda^i_{\alpha}\lambda^j_{\beta} = 0 \quad (\alpha \neq \beta), \tag{1.10}$$

where the e's have values $+1$ or -1, depending upon the character of the form (1.1). The directions determined by λ^i_{α} are called the Ricci principal directions of V_n.

The roots of (1.8) are scalars and by the above observation we have for each root

$$\rho(x') = \rho(x), \tag{1.11}$$

from which follows

$$\xi^i \frac{\partial \rho}{\partial x^i} = 0. \tag{1.12}$$

The components λ^i_{α}, being functions of the g's and their derivatives and being uniquely determined (since they are unit vectors) at each point of V_n we have

$$\lambda^i_{\alpha}(x') = \lambda^j_{\alpha}(x) \frac{\partial x'^i}{\partial x^j}, \tag{1.13}$$

that is the ennuples of vectors along a trajectory of a motion are brought into coincidence by the motion. From (1.13) and (1.4) we have

$$\xi^k \frac{\partial \lambda^i_{\alpha}}{\partial x^k} - \lambda^j_{\alpha} \frac{\partial \xi^i}{\partial x^j} = 0. \tag{1.14}$$

Suppose next that all the roots of (1.8) are not simple. If ρ is a root of multiplicity r, then r unit vectors of components λ^i_{σ} ($\sigma = 1, \cdots, r$) exist satisfying (1.9), mutually orthogonal to one another, and orthogonal to the vectors corresponding to the other roots.[4] These vectors are determined to within a matrix t^{σ}_{τ} for which

$$\sum_{\tau} e_{\tau} t^{\tau}_{\sigma} t^{\tau}_{\sigma} = \bar{e}_{\sigma}, \qquad \sum_{\tau} e_{\tau} e^{\tau}_{\rho} e^{\tau}_{\sigma} = 0 \qquad (\rho, \sigma, \tau = 1, \cdots, r;\ \rho \neq \sigma),$$

[4] R. G., pp. 108–114.

in the sense that

$$\bar{\lambda}^i_\sigma = t^\tau_\sigma \lambda^i_\tau$$

are the components of orthogonal unit vectors satisfying (1.9). Hence in this case in place of equations (1.13) we may have

$$\lambda^i_\sigma(x') = t^\tau_\sigma(x')\lambda^j_\tau(x)\frac{\partial x'^i}{\partial x^j}, \tag{1.15}$$

or for an infinitestimal motion (1.4)

$$\lambda^i_\sigma(x) + \frac{\partial \lambda^i_\sigma}{\partial x^j}\xi^j\delta t = \sum_\tau (\delta^\tau_\sigma + e_\tau \gamma^\tau_\sigma \delta t)\lambda^j_\tau(x)\left(\delta^i_j + \frac{\partial \xi^i}{\partial x^j}\delta t\right), \tag{1.16}$$

from which we have

$$\xi^j\frac{\partial \lambda^i_\sigma}{\partial x^j} - \lambda^j_\sigma\frac{\partial \xi^i}{\partial x^j} = \sum_\tau e_\tau \gamma^\tau_\sigma \lambda^i_\tau. \tag{1.17}$$

Expressing the condition that the vectors λ^i_σ be unit vectors, that is (1.10), and making use of (1.5), we find that

$$\gamma^\tau_\sigma + \gamma^\sigma_\tau = 0. \tag{1.18}$$

Incidentally we have (1.14) from (1.17) when ρ is a simple root, since from (1.18) we have $\gamma^\sigma_\sigma = 0$. When we have (1.16) holding, the motion may be looked upon as consisting of a translation and a rotation, the quantities $\gamma^\sigma_\tau\delta t$ being the components of rotation.

If we denote by λ^α_i the covariant components of λ^i_α, that is

$$\lambda^\alpha_i = g_{ij}\lambda^j_\alpha, \tag{1.19}$$

we have in consequence of (1.10)

$$\lambda^i_\alpha\lambda^\alpha_i = e_\alpha \ (\alpha \text{ not summed}), \quad \lambda^i_\alpha\lambda^\beta_i = 0 \ (\alpha \neq \beta), \quad \sum_\alpha e_\alpha \lambda^\alpha_i \lambda^\alpha_j = g_{ij}, \tag{1.20}$$

and

$$g_{ij} = \sum_\alpha e_\alpha \lambda^\alpha_i \lambda^\alpha_j.\text{[5]} \tag{1.21}$$

Hence for any infinitesimal motion of vector ξ^i we have from (1.17) for the determination of γ^τ_σ the result

$$\gamma^\tau_\sigma = \lambda^\tau_i\left(\xi^j\frac{\partial \lambda^i_\sigma}{\partial x^j} - \lambda^k_\sigma\frac{\partial \xi^i}{\partial x^k}\right). \tag{1.22}$$

2. In this and the next section we consider the case when the roots of equation (1.8) are simple. Equations (1.14) may be written in the form

$$\frac{\partial \xi^i}{\partial x^j} + \xi^k L^i_{kj} = 0, \tag{2.1}$$

[5] Cf. R. G., p. 96.

where by definition, on making use of (1.20),

$$L^i_{kj} = \sum_\alpha e_\alpha \lambda^i_\alpha \frac{\partial \lambda^\alpha_j}{\partial x^k} = -\sum_\alpha e_\alpha \lambda^\alpha_j \frac{\partial \lambda^i_\alpha}{\partial x^k}, \tag{2.2}$$

from which it follows that

$$\frac{\partial \lambda^i_\alpha}{\partial x^j} + \lambda^k_\alpha L^i_{jk} = 0, \qquad \frac{\partial \lambda^\alpha_i}{\partial x^j} - \lambda^\alpha_k L^k_{ji} = 0. \tag{2.3}$$

We write (2.1) as follows

$$\xi^i_{/j} = 0, \tag{2.4}$$

and say that a solidus followed by an index indicates covariant differentiation with respect to the asymmetric connection of coefficients L^i_{jk}.[6] With respect to this connection the vectors of the vector-field ξ^i form a parallel field.[7]

Expressing the condition of integrability of (2.1) we have

$$\xi^i L^h_{ijk} = 0, \tag{2.5}$$

where

$$L^h_{ijk} = \frac{\partial L^h_{ik}}{\partial x^j} - \frac{\partial L^h_{ij}}{\partial x^k} + L^l_{ik} L^h_{lj} - L^l_{ij} L^h_{lk}.\text{[8]} \tag{2.6}$$

A solution of (2.1) must satisfy (2.5) and the equations resulting from (2.5) by successive covariant differentiation; these reduce by (2.4) to

$$\begin{gathered} \xi^i L^h_{ijk/m_1} = 0, \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ \xi^i L^h_{ijk/m_1 \cdots m_q} = 0, \\ \cdots\cdots\cdots\cdots\cdots \end{gathered} \tag{2.7}$$

It can be shown[9] that in order that (2.1) admit a solution it is necessary and sufficient that there exist a number q such that the rank of the matrix of equations (2.5) and (2.7) be $n - r$ (>0) and that this be also the rank of the augmented matrix when one more set of equations is added by covariant differentiation; and that when this condition is satisfied, the equations (2.1) admit r sets of solutions ξ^i_ν such that the rank of the matrix $\| \xi^i_\nu \|$ is r, any other solution being a linear combination with constant coefficients of these r solutions. Since the equations (2.1) are linear and homogeneous in the ξ's, the r sets of solutions generate a group G_r. Hence we have:

[6] N. R. G., p. 5–7; this reference is to the author's *Non-Riemannian Geometry*.
[7] N. R. G., p. 19.
[8] N. R. G., p. 19.
[9] N. R. G., p. 20.

When a V_n, for which the roots of (1.8) *are simple, admits motions, the complete group G_r of its motions is such that the rank of the matrix $\| \xi^i_\nu \|$ of G_r is r.*

3. We shall show conversely that

When a V_n admits a complete group G_r of motions for which the rank of the matrix $\| \xi^i_\nu \|$ is r, the vectors ξ^i_ν satisfy (1.14) *in which λ^i_α are the components of unit vectors determining the Ricci principal directions of the space.*

If $r < n$, a coördinate system exists in terms of which

$$\xi^s_\nu = 0 \qquad (s = r + 1, \cdots, n).\text{[10]} \tag{3.1}$$

Since the determinant of ξ^a_ν for $a = 1, \cdots, r$ is not zero, functions ξ^ν_a are uniquely determined by

$$\xi^a_\nu \xi^\nu_b = \delta^a_b, \qquad \xi^a_\nu \xi^\mu_a = \delta^\mu_\nu \qquad (a, b, \mu, \nu = 1, \cdots, r). \tag{3.2}$$

We define functions Λ^i_{jb} by

$$\Lambda^a_{jb} = \xi^a_\nu \frac{\partial \xi^\nu_b}{\partial x^j} = -\xi^\nu_b \frac{\partial \xi^a_\nu}{\partial x^j}, \qquad \Lambda^s_{jb} = 0 \quad (s = r + 1, \cdots, n; j = 1, \cdots, n), \tag{3.3}$$

from which we have

$$\frac{\partial \xi^a_\nu}{\partial x^j} + \xi^b_\nu \Lambda^a_{jb} = 0, \qquad \frac{\partial \xi^\nu_a}{\partial x^j} - \xi^\nu_b \Lambda^b_{ja}. \tag{3.4}$$

Equations (1.14) are equivalent to

$$\frac{\partial \lambda^i_\alpha}{\partial x^b} + \lambda^j_\alpha \Lambda^i_{jb} = 0 \qquad (i, j = 1, \cdots, n; b = 1, \cdots, r). \tag{3.5}$$

The conditions of integrability of these equations are

$$\lambda^j_\alpha \Lambda^i_{jbc} = 0,$$

where Λ^i_{jbc} are the same functions of the Λ's as L^i_{jkl} are of the L's. When $i = r + 1, \cdots, n$ the quantities Λ^i_{jbc} are identically zero because of the second set of equations (3.3); when $i = 1, \cdots, r$, they can be shown to be zero.[11] Hence the system (3.5) is completely integrable, and a solution is defined by taking as initial values for $x^1 = \cdots = x^r = 0$ arbitrary functions of $x^{r+1}, \cdots, x^n$; when $r = n$ these are arbitrary constants. We shall show how they may be chosen so that the λ's determine Ricci directions. A necessary and sufficient condition for this to be the case is that (1.10) and

$$R_{ij} \lambda^i_\alpha \lambda^j_\beta = 0 \qquad (\alpha \neq \beta) \tag{3.6}$$

be satisfied. For, if this condition is satisfied and we define quantities ρ_α by $R_{ij} \lambda^i_\alpha \lambda^j_\alpha = e_\alpha \rho_\alpha$, then λ^i_α satisfy (1.9) and ρ_α are the roots of (1.8).

---

[10] Cf. C. G., p. 74.

[11] C. G., p. 76, equations (21.19).

In consequence of (3.1), (3.4) and the fact that $\| \xi^a_\nu \|$ is of rank r we have from (1.5) and (1.7)

$$
(3.7)\qquad
\begin{aligned}
&\frac{\partial g_{ij}}{\partial x^a} - g_{ib}\Lambda^b_{ja} - g_{bj}\Lambda^b_{ia} = 0\,,\\
&\frac{\partial R_{ij}}{\partial x^a} - R_{ib}\Lambda^b_{ja} - R_{bj}\Lambda^b_{ia} = 0 \qquad (i, j = 1, \cdots, n; a, b = 1, \cdots, r).
\end{aligned}
$$

Consequently, if λ^i_α and λ^i_β are any two solutions of (3.5), we have

$$
(3.8)\qquad \frac{\partial}{\partial x^a}(g_{ij}\lambda^i_\alpha\lambda^j_\alpha) = 0\,, \qquad \frac{\partial}{\partial x^a}(g_{ij}\lambda^i_\alpha\lambda^j_\beta) = 0\,, \qquad \frac{\partial}{\partial x^a}(R_{ij}\lambda^i_\alpha\lambda^j_\beta) = 0\,.
$$

Accordingly, if we choose the initial values of the λ's so as to satisfy (1.10) and (3.6), these equations will be satisfied by the corresponding solution for all values of the x's. This choice is given by finding an orthogonal ennuple of unit vectors satisfying (1.8) after putting $x^1 = \cdots = x^r = 0$, and thus the theorem is proved. When in particular $r = n$, that is when the group is simply transitive, the λ's are the vectors of the reciprocal simply transitive group.[12]

It should be remarked that in the preceding discussion the question of whether the roots of equation (1.8) are simple or not is not involved, so that the converse theorem applies to a space for which there are multiple roots, if the space admits a G_r for which the rank of $\| \xi^i_\nu \|$ is r.

If we put

$$
(3.9)\qquad \lambda'^{\,i}_\alpha = c^\beta_\alpha\lambda^i_\beta\,,
$$

where the c's are constants subject to the conditions

$$
\sum_\beta e_\beta c^\beta_\alpha c^\beta_\alpha = e'_\alpha, \qquad \sum_\beta e_\beta c^\beta_\alpha c^\beta_\gamma = 0 \qquad (\alpha \neq \gamma),
$$

$\lambda'^{\,i}_\alpha$ are the components of an orthogonal ennuple of unit vectors; they satisfy (3.5) but not necessarily (3.6), and consequently they do not determine the Ricci directions for arbitrary values of the c's.

If we have an orthogonal ennuple of unit vectors and differentiate the corresponding equation (1.21) with respect to x^k and make use of (2.3), we obtain

$$
(3.10)\qquad \frac{\partial g_{ij}}{\partial x^k} - g_{ih}L^h_{kj} - g_{hj}L^h_{ki} = 0\,.
$$

If the vectors λ^i_α are such that equations (2.1) admit a solution, then from (2.1) and (3.10) we obtain the Killing equations (1.5), and consequently V_n admits a G_1 of motions. Since (1.14) and (3.5) are equivalent, we have equations (1.14) holding and consequently all the results of §2. Hence we have:

If a V_n admits an orthogonal ennuple of unit vectors for which equations (2.1)

[12] C. G., pp. 113–115.

admit a complete set of r ($\geqq 1$) *solutions, then* V_n *admits a group* G_r *of motions and the rank of the matrix* $\| \xi^i_\nu \|$ *is* r.

From the preceding results we have that either λ^i_α determine the Ricci directions or suitable linear combinations with constant coefficients determine these directions.

4. We consider in this section groups of motion G_r for which the rank of the matrix $\| \xi^i_\alpha \|$ is q, less than r. We assume without loss of generality that ξ^i_ν for $\nu = 1, \cdots, q$ are independent and put

$$\xi^i_\sigma = \varphi^\nu_\sigma \xi^i_\nu \qquad (\sigma = q + 1, \cdots, r). \tag{4.1}$$

It follows from (1.5) and (1.7) that

$$\xi^k_\nu \left(g_{ik} \frac{\partial \varphi^\nu_\sigma}{\partial x^j} + g_{jk} \frac{\partial \varphi^\nu_\sigma}{\partial x^i} \right) = 0, \tag{4.2}$$

$$\xi^k_\nu \left(R_{ik} \frac{\partial \varphi^\nu_\sigma}{\partial x^j} + R_{jk} \frac{\partial \varphi^\nu_\sigma}{\partial x^i} \right) = 0 \qquad (i, j, = 1, \cdots, n). \tag{4.3}$$

If we put

$$g_{ik} \xi^k_\nu \frac{\partial \varphi^\nu_\sigma}{\partial x^j} = \varphi_{\sigma ji}, \tag{4.4}$$

equations (4.2) become

$$\varphi_{\sigma ji} + \varphi_{\sigma ij} = 0, \tag{4.5}$$

so that for each value of σ we have a skew-symmetric covariant tensor of the second order. Equations (4.3) may be written

$$R^h_i \varphi_{\sigma jh} + R^h_j \varphi_{\sigma ih} = 0. \tag{4.6}$$

A coördinate system can be chosen so that at an arbitrary point P we have $g_{ij} = R_{ij} = R^j_i = 0$ ($i \neq j$), in which case at P equations (4.6) become, in consequence of (4.5),

$$(R^i_i - R^j_j) \varphi_{\sigma ji} = 0. \tag{4.7}$$

Since for each value of σ not all of the quantities φ^ν_σ are constants, it follows from (4.4) that not all of the quantities $\varphi_{\sigma ji}$ can be zero. Hence for a certain i and j, we have $R^i_i = R^j_j$, that is

$$\frac{R_{ii}}{g_{ii}} = \frac{R_{jj}}{g_{jj}},$$

and consequently at least two of the roots of (1.8) are equal at P. Since P is an arbitrary point, it follows that at least two of the roots of (1.8) are equal and we have

When a V_n *admits a group* G_r *of motions, for which the rank of the matrix of the*

vectors $\| \xi^i_\alpha \|$ *is less than* r, *not all the roots of the characteristic equation* (1.8) *are simple, that is not all the Ricci principal directions are uniquely determined.*

Also it follows that if the generic rank of the matrix $\varphi_{\sigma ji}$ is p and P is a point for which the rank is p, we may determine the number of multiple roots and their multiplicity.

We recall that for a G_r of the kind under discussion equations (1.5) for the q vectors ξ^i_ν and equations (4.2) constitute a necessary and sufficient condition that the g's must satisfy in order that G_r be a group of motions, in addition to the requirement that the determinant of the g's is different from zero. There are $(r - q)\ N$ (where $N = \frac{1}{2}n(n+1)$) equations (4.2) linear and homogeneous in the N quantities g_{ij}. Hence the rank of the matrix of these equations must be less than N. If it is $N - 1$, it follows from (4.3) that $R_{ij} = \rho g_{ij}$ that is V_n is an Einstein space.

5. If the components g_{ij} of a tensor satisfy (1.5) and (4.2) so also do $e^{2\sigma} g_{ij}$, provided that

$$\xi^i_\nu \frac{\partial \sigma}{\partial x^i} = 0 \qquad (\nu = 1, \cdots, q). \tag{5.1}$$

Only when $q < n$ is the $\bar{V}_n$ with the fundamental tensor $e^{2\sigma} g_{ij}$ different from V_n.[13] If a comma followed by one or more indices indicates covariant differentiation with respect to the g's and we put

$$\sigma_{ij} = \sigma_{,ij} - \sigma_{,i}\sigma_{,j}\,, \tag{5.2}$$

the components $\bar{R}_{ij}$ of the Ricci tensor for $\bar{V}_n$ are given by[14]

$$\bar{R}_{ij} = R_{ij} + (n-2)\sigma_{ij} + g_{ij}[\Delta_2\sigma + (n-2)\Delta_1\sigma]. \tag{5.3}$$

Expressing the condition that these satisfy (1.7), we obtain in consequence of (1.5) and (1.7),

$$(n-2)A_{\nu ij} + g_{ij}\xi^k_\nu \frac{\partial}{\partial x^k}[\Delta_2\sigma + (n-2)\Delta_1\sigma] = 0, \tag{5.4}$$

where

$$\begin{aligned} A_{\nu ij} &\equiv \xi^k_\nu \frac{\partial \sigma_{ij}}{\partial x^k} + \sigma_{ih}\frac{\partial \xi^h_\nu}{\partial x^j} + \sigma_{jh}\frac{\partial \xi^h_\nu}{\partial x^i} \\ &= \xi^k_\nu \sigma_{ij,k} + \sigma_{ih}\xi^h_{\nu,j} + \sigma_{jh}\xi^h_{\nu,i}. \end{aligned} \tag{5.5}$$

From (5.1) we have

$$\xi^k_\nu \sigma_{,ki} + \xi^k_{\nu,i}\sigma_{,k} = 0. \tag{5.6}$$

---

[13] Cf. Knebelman, *On groups of motions in related spaces*, American Journal of Mathematics, Vol. 52 (1930), p. 282.

[14] R. G., p. 90.

In consequence of (5.2) and (5.6) we have from (5.5)

$$A_{\nu ij} = \xi^k_\nu \sigma_{,ijk} + \sigma_{,ih}\xi^h_{\nu,j} + \sigma_{,jh}\xi^h_{\nu,i}. \tag{5.7}$$

From (5.6) we have by covariant differentiation

$$\xi^k_\nu \sigma_{,ikj} + \xi^k_{\nu,j}\sigma_{,ik} + \xi^k_{\nu,ij}\sigma_{,k} + \xi^k_{\nu,i}\sigma_{,jk} = 0,$$

by means of which and the equations

$$\xi^k_{\nu,ij} = \xi^h_\nu R^k_{ijh} \tag{5.8}$$ [15]

equations (5.7) are reducible to

$$A_{\nu ij} = \xi^k_\nu(\sigma_{,ijk} - \sigma_{,ikj} - \sigma_{,h}R^h_{ijk}).$$

In view of the Ricci identities[16] we have that the quantities $A_{\nu ij}$ are zero, in consequence of which and (5.6) equations (1.5) are satisfied by $\sigma_{,ij} - \varphi\sigma_{,i}\sigma_{,j}$, where φ is a constant or any solution of the system (5.1).

From (1.5) we have

$$\xi^k_\nu \frac{\partial g^{ij}}{\partial x^k} - g^{hi}\frac{\partial \xi^j_\nu}{\partial x^h} - g^{hj}\frac{\partial \xi^i_\nu}{\partial x^h} = 0,$$

which because of the identity $g^{ij}{}_{,k} = 0$ is equivalent to

$$g^{hi}\xi^j_{\nu,h} + g^{hj}\xi^i_{\nu,h} = 0. \tag{5.9}$$

In consequence of these equations and (5.6) we have

$$\xi^k_\nu \frac{\partial}{\partial x^k}\Delta_1\sigma = \xi^k_\nu \frac{\partial}{\partial x^k}(g^{ij}\sigma_{,i}\sigma_{,j}) = 0.$$

Also because of (5.9) and the fact that the right-hand member of (5.7) is zero we find that

$$\xi^k_\nu \frac{\partial}{\partial x^k}\Delta_2\sigma = \xi^k_\nu \frac{\partial}{\partial x^k}(g^{ij}\sigma_{,ij}) = 0.$$

Accordingly equations (5.4) are satisfied.

If $q < r$, equations (4.2) are satisfied by $e^{2\sigma}g_{ij}$ and the equations (4.3) for $\bar{V}_n$, in consequence of (5.3) require that

$$\xi^k_\nu\left(\sigma_{,ik}\frac{\partial \varphi^\nu_\sigma}{\partial x^j} + \sigma_{,jk}\frac{\partial \varphi^\nu_\sigma}{\partial x^i}\right) = 0. \tag{5.10}$$

In order to verify this we remark that $\xi^k_\sigma = \varphi^\nu_\sigma \xi^k_\nu$ must satisfy (5.8); this leads to the conditions

$$\varphi^\nu_{\sigma,ij}\xi^k_\nu + \varphi^\nu_{\sigma,i}\xi^k_{\nu,j} + \varphi^\nu_{\sigma,j}\xi^k_{\nu,i} = 0.$$

[15] C. G., p. 216, Ex. 3.
[16] R. G., p. 30.

Multiplying by $\sigma_{,k}$ and summing for k, the resulting equation is reducible to (5.10) because of (5.1) and (5.6).

As a result of the foregoing investigation we have

When a V_n with fundamental tensor g_{ij} admits an intransitive group of motions, the same group is a group of motions of the space with the fundamental tensor $\bar{g}_{ij} = \sigma_{,ij} - \varphi\sigma_{,i}\sigma_{,j}$, where σ is any solution of (5.1) *and φ is a solution of* (5.1) *such that the matrix $\| \bar{g}_{ij} \|$ is of rank n.*

PRINCETON UNIVERSITY.

Annals of Mathematics
Vol. 36, No. 4, October, 1935

ON CERTAIN AREA-PRESERVING MAPS[1]

By A. B. Brown and M. Halperin

(Received January 1, 1934)

In this paper the authors obtain characterizations of wide classes of area-preserving transformations of a simply-connected region into a circular region, and extend some of the results to curved surfaces and to volumes.[2]

Theorem 1. *Let $\mathfrak{S}$ be a family of nested simple closed curves which fill the the simply-connected plane region A of finite area;*[3] *O the point interior to each curve of $\mathfrak{S}$; Γ a Jordan arc which meets each curve of $\mathfrak{S}$ in a single point. Let $\mathfrak{S}$ have a representation of the form*

$$f(x, y) = a, \tag{1}$$

where f has continuous first partial derivatives except at O, not both zero. Let C be a circle enclosing a plane region A' of area equal to that of A.

Then there exists an area-preserving homeomorphism which maps A upon A', the curves of $\mathfrak{S}$ upon circles concentric with C, and Γ upon a given radius of C. Except for a possible reflection, the map is unique.

It is easily shown that a permissible change in the function f will make the area, say $\mathbf{A}(a)$, enclosed by the curve of $\mathfrak{S}$ for any value of a, be πa^2:[4]

$$\mathbf{A}(a) = \pi a^2. \tag{2}$$

Let (R, Θ) be polar coördinates in a system with pole at the center of C and with the polar axis along the given radius of C. We define a transformation by (3) and (4), where we note that points on a curve of $\mathfrak{S}$ are mapped on points of the circle concentric with C and enclosing the same area πa^2.

$$R = f(x, y) \tag{3}$$

$$\Theta = (1/f) \int_{\gamma(x,y)}^{(x,y)} \frac{ds}{f_n} = (1/f) \int_{\gamma}^{(x,y)} \frac{ds}{(f_x^2 + f_x^2)^{1/2}},\text{[5]} \tag{4}$$

---

[1] Presented to the American Mathematical Society, March 31, 1934.

[2] F. Schellhammer wrote a paper on the same general subject: *Über äquivalente Abbildung*, Zeitschrift für Math. und Phys. 23 (1878), pp. 69–84. He treats simply-connected regions whose boundaries are cut by each line of a family of parallel lines in just two points. He has nothing like our characterizations of the maps by means of families of curves. Our first theorem characterizes, among others, all area-preserving maps of A on A' which are expressed in Cartesian coördinates by means of functions having continuous first partial derivatives.

[3] With a slight change in the wording of the theorem, and of the proof, the restriction to finite area can be removed.

[4] This means that $[f(x,y)]^2$ equals $1/\pi$ times the area interior to the curve of $\mathfrak{S}$ through (x, y).

[5] A subscript for f denotes partial differentiation.

where $Y(x, y)$ is the point of intersection with Γ of the curve of $\mathfrak{S}$ through (x, y), f_n is the directional derivative in the outer normal direction, and the integral is evaluated along the curve of $\mathfrak{S}$ with s measured in the sense for which the interior is on the left. The functions R, Θ are then continuous at all points of A, except at O in the case of Θ. From (3) and (4) it is easily seen that the map is one-to-one and continuous between A and A' except for possible overlapping through Θ's becoming greater than 2π, or possible non-covering due to Θ's not reaching the value 2π.

Let $u(R)$ be the area of the region in A bounded by the four curves corresponding to $\Theta = \Theta_1, \Theta = \Theta_2$, $R = R_1$ and $R = R$, $0 \leqq \Theta_1 < \Theta_2 \leqq 2\pi$, where we take Θ_2 small enough so that such curves exist. We shall show below that this is no restriction. Let P_1 and P_2 denote the points in A corresponding to (R, Θ_1) and (R, Θ_2).

$$du/dR = \int_{P_1}^{P_2} \frac{ds}{f_n} = R(\Theta_2 - \Theta_1). \tag{5}$$

The derivation, which we omit, of the first equality in (5) involves the relations

$$\iint dx\,dy = \iint \frac{df\,dy}{f_x} = - \iint \frac{df\,dx}{f_y},$$

$$dy/f_x = - dy/f_y = ds/f_n, \quad \text{on curves of } \mathfrak{S},$$

and the fact that du/dR is unchanged if the curves corresponding to $\Theta = \Theta_1$ and $\Theta = \Theta_2$ are replaced by other curves through P_1 and P_2 respectively, each of which meets each curve of $\mathfrak{S}$ in a single point. The second equality in (5) follows from (4) and (3).

From (5) we have

$$u = \tfrac{1}{2}(R^2 - R_1^2)(\Theta_2 - \Theta_1),$$

which equals the corresponding area in A'. Consequently the map is area-preserving.

If P_1 and P_2 are both on Γ, then since for the purposes of finding du/dR we may use Γ as a boundary twice, it follows from (1), (2) and (3) that $u = \pi(R^2 - R_1^2)$. Therefore $du/dR = 2\pi R$, and from (5) we find that $\Theta_2 = \Theta_2 - \Theta_1 = 2\pi$. Hence the map is one-to-one between all of A and all of A'.

Similar considerations show that the only area-preserving maps of a circle-interior on itself which keep a given radius fixed and transform into itself each circle concentric with the given circle, are the identity and a reflection. Hence the uniqueness condition is satisfied, and the proof is complete.

THEOREM 2. *Let B be a simply-connected region of finite area on a surface S having a metric given by*

$$ds^2 = Ed\alpha^2 + 2Fd\alpha d\beta + Gd\beta^2,$$

where E, F and G are continuous and $EG - F^2 \neq 0$ in B. Then if, in Theorem 1 B is substituted for A, and (α, β) substituted for (x, y), the resulting theorem is true.

The proof is like that of Theorem 1 except that (x, y) is replaced by (α, β); $f_n = (f_x^2 + f_y^2)^{\frac{1}{2}}$ is replaced by $(\Delta_1 f)^{\frac{1}{2}}$, where $\Delta_1 f$ is the differential invariant

$$\Delta_1 f = \frac{Ef_\beta^2 - 2Ff_\alpha f_\beta + Gf_\alpha^2}{EG - F^2};$$

and the derivation of (5) is somewhat lengthier. We give no further details.

For the plane case (Theorem 1), conformal mapping shows the existence of such families $\mathfrak{S}$ for any simply-connected region A of finite area. Under certain restrictions a similar statement can be made in the case of a curved surface. In the following theorem, however, the hypotheses may be too stringent to be satisfied by the most general region A even when planar, but the conclusion is interesting in that in this case the map is characterized merely by a single family of curves.

THEOREM 3. *Under the hypotheses of Theorem 2, let* $\mathbf{G}$ *be a one-parameter family of curves of bounded length in* B, *homeomorphic to a family of parallel chords in* A'. *Suppose a function* $g(\alpha, \beta)$ *is defined in* B *such that*:

(a) g *is constant along each curve of* $\mathbf{G}$;

(b) *the area on a particular side of the curve* $g(\alpha, \beta) = c$, *is* c;

(c) g *has continuous first partial derivatives, not both zero, throughout* B;

(d) $\Delta_1 g > k > 0$, k *constant for all of* B.

Suppose also that the locus Γ *of one set of end-points of the curves of* $\mathbf{G}$ *is given by equating* α *and* β *to continuous functions of* c (*the constant in the equation* $g = c$). *Then there exists an area-preserving homeomorphism of* B *with* A', *which maps* $\mathbf{G}$ *upon any given family of parallel chords of* A'. *This homeomorphism is unique except for two possible reflections.*

PROOF: One such transformation is given by the following equations, where C, the boundary of A', is (permissibly) taken as the unit circle with center at the origin, in an (X, Y)-plane, and $X(\alpha, \beta)$ in the second equation is the function determined by the first equation:

$$X[(1 - X^2)]^{\frac{1}{2}} + \cos^{-1}(-X) = g(\alpha, \beta), \qquad 0 < \cos^{-1}(-X) < \pi,$$

$$Y = \int_Y^{(\alpha,\beta)} \frac{ds}{[\Delta_1 X(\alpha, \beta)]^{\frac{1}{2}}} - (1 - X^2)^{\frac{1}{2}}, \qquad Y \text{ on } \Gamma.$$

The remainder of the proof is similar to the proofs of the preceding theorems, and is omitted.

We now present a result for the three-dimensional case similar to Theorem 1. Similar results hold for spaces of higher dimensions.

THEOREM 4. *Let there exist in an* (x, y, z) *number-space, a configuration* Λ, *which is a homeomorph of a configuration* Λ' *consisting of*:

(a) A', *the interior of an ordinary sphere with center at the origin, in a number-space with spherical coördinates* (R, Φ, Θ);

(b) $\mathbf{S}'$, *the spheres* $R = k$, *in* A';

(c) $\mathbf{C}'$, *the intersections of* $\mathbf{S}'$ *with the half-cones* $\Phi = m$;

(d) p', *the part in* A' *of the half-plane* $\Theta = 0$.

Let A, O, $\mathbf{S}$, $\mathbf{C}$, p and ζ be the respective homologs in Λ of A', the origin, $\mathbf{S}'$, $\mathbf{C}'$, p' and the ray $\Phi = 0$, in Λ'; with the volume of A equal to that of A'. Suppose that the surfaces $\mathbf{S}$ have a representation of the form

$$(6) \qquad H(x, y, z) = a\,,$$

and that the curves $\mathbf{C}$ have a representation given by (6) *and*

$$(7) \qquad K(x, y, z) = b\,.$$

We assume that H and K have continuous first partial derivatives and that the matrix of the first partial derivatives is of rank 2, *at all points of A except images of the points on the rays $\Phi = 0, \pi$.*

Then there exists a volume-preserving homeomorphism which maps A, $\mathbf{S}$, $\mathbf{C}$, p upon A', $\mathbf{S}'$, $\mathbf{C}'$, p', respectively. This map is unique except for certain reflections.

PROOF: We may assume that H is such that the volume enclosed by the surface (6) for any a is $(4/3)\pi a^3$. Given any point Q of A, for the present suppose it does not lie on the homologs of the rays $\Phi = 0, \pi$. Let $C(Q)$ be the curve of $\mathbf{C}$ through Q. Then C divides the surface, say $S(Q)$, of $\mathbf{S}$ on which it lies into two regions, one of which, say $M(Q)$, contains a point of ζ. Let σ denote area in $M(Q)$. A volume-preserving homeomorphism is then determined by letting Q correspond to (R, Φ, Θ) as determined by (8), (9), (10), with the supplementary definitions below.

$$(8) \qquad R = H(x, y, z)\,.$$

$$(9) \qquad 1 - \cos\Phi = (1/2\pi H^2)\int_{M(Q)} \frac{d\sigma}{H_n}\,, \qquad 0 < \Phi < \pi\,;$$

$$(10) \qquad \Theta = (1/H^2 \sin\Phi)\int_{Q_1}^{Q} \frac{ds}{(H_n)[\Delta_1\Phi(x, y, z)]^{\frac{1}{2}}} \quad \text{along } C(Q),\, Q_1 \text{ on } p\,.$$

Here H_n is the directional derivative in the outer normal direction; $\Delta_1\Phi$ is with respect to $S(Q)$; $\Phi(x, y, z)$ is the function determined by (9); and the integral in (10) is in the sense for which Θ increases on the corresponding curve of $\mathbf{C}'$.

For points of A corresponding to points of A' on the rays $\Phi = 0, \pi$, we keep (8) as it is, replace (9) by the equation $\Phi = 0, \pi$ as the case may be, and dispense with (10), which becomes unnecessary.

The details of the proof are omitted. They are of the same nature as those for Theorem 1.

A special case for the region A in the plane case is mentioned as interesting because of a very easily defined map. Given a curve $r = f(\theta) > 0$, $0 \leqq \theta \leqq 2\pi$, $f(2\pi) = f(0)$, with (r, θ) as polar coördinates, enclosing an area π, we apply the transformation

$$R = r/f(\theta)\,, \qquad \Theta = \int_0^\theta [f(\theta)]^2\, d\theta\,,$$

with (R, Θ) polar coördinates of the transformed point. The preservation of area is easily established by first considering regions in the transform of A bounded by arcs of concentric circles and radii cut off by these circles.

The following example shows that our restrictions on the nature of the family $\mathfrak{S}$ in Theorem 1 are not superfluous. The curves of $\mathfrak{S}$ are circles, of radii r, $0 < r < 2$. When $r \leqq 1$, the center is at the origin; when $r \geqq 1$, the center is at the point $x = \frac{1}{2}(r - 1)$, $y = 0$. It is easily verified that in this case the conclusion of Theorem 1 cannot be satisfied. The difficulty arises at the circle $r = 1$.

COLUMBIA UNIVERSITY.

ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

THREE EXAMPLES IN THE THEORY OF FOURIER SERIES[1]

BY W. C. RANDELS

(Received May 7, 1934)

1. **Introduction.** This paper consists of three notes each of which may be read separately. The notation used is familiar and will only be reviewed briefly. We shall use $f(x)$ to mean an integrable function which is periodic of period 2π. We shall make use of the following functions.

$$\varphi(t) = f(x + t) + f(x - t) - 2f(x), \tag{1}$$

$$\psi(t) = f(x + t) - f(x - t), \tag{2}$$

$$\chi(t) = f(x + t) - f(x - t) - 2tf'(x), \tag{3}$$

$$\Phi(t) = \int_0^t |\varphi(\tau)| \, d\tau, \tag{4}$$

$$\Psi(t) = \int_0^t |\psi(\tau)| \, d\tau, \tag{5}$$

$$\varphi_1(t) = \int_0^t \varphi(\tau) \, d\tau, \tag{6}$$

$$\varphi_0(t) = \int_0^t |d\varphi(\tau)|, \tag{7}$$

$$\chi_0(t) = \int_0^t |d\chi(\tau)|, \tag{8}$$

$$\bar{f}(x) = \lim_{\epsilon \to 0} -\frac{1}{2\pi} \int_\epsilon^\pi \psi(t) \cot t/2 \, dt, \tag{9}$$

$$\bar{f}'(x) = \lim_{\epsilon \to 0} -\frac{1}{4\pi} \int_\epsilon^\pi \varphi(t)(\sin t/2)^{-2} \, dt. \tag{10}$$

By $\int_0^t |d\varphi(\tau)|$ we mean the total variation of $\varphi(t)$ on the interval $(0, t)$. The function $\bar{f}(x)$ exists and is finite almost everywhere, and, if $f(x)$ is of bounded variation on $(-\pi, \pi)$, $\bar{f}'(x)$ exists and is finite almost everywhere. We also use an alternative expression for $\bar{f}(x)$,

$$\bar{f}(x) = \lim_{\epsilon \to 0} -\frac{1}{\pi} \int_\epsilon^\infty \psi(t) \frac{dt}{t}. \tag{11}$$

---

[1] The author is indebted to Prof. J. D. Tamarkin for his criticism and suggestions.

We shall consider four classes, of trigonometric series and their related sum functions. We indicate these classes by L, $\bar{L}$, L', and $\bar{L}'$. The class L is the class of Fourier series and functions integrable over $(-\pi, \pi)$. We write

$$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx) \tag{12}$$

where

$$a_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos nx \, dx, \qquad b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin nx \, dx .$$

The conjugate series of $f(x)$ is

$$\sum_{n=1}^{\infty} (a_n \sin nx - b_n \cos nx) \tag{13}$$

and the corresponding sum function is $\bar{f}(x)$. The class of such series and functions is denoted by $\bar{L}$. If $f(x)$ is of bounded variation over $(-\pi, \pi)$ the series

$$\sum_{n=1}^{\infty} n(- a_n \sin nx + b_n \cos nx) \tag{14}$$

$$\sum_{n=1}^{\infty} n(a_n \cos nx + b_n \sin nx) \tag{15}$$

are members of the classes L' and $\bar{L}'$ respectively. The corresponding sum functions are $f'(x)$ and $\bar{f}'(x)$.

We denote by $\mathfrak{T}$ any one of the four classes of series defined above. The general term of a series of class $\mathfrak{T}$ is called $A_n(x)$ and the sum function associated with the series is called $F(x)$. We define

$$F_n(x) \equiv \sum_{\nu=0}^{n} A_\nu(x) . \tag{16}$$

In the case $\mathfrak{T} = L, \bar{L}, L'$, and $\bar{L}'$, $F_n(x)$ is written $S_n(x)$, $\bar{S}_n(X)$, $S_n'(x)$ and $\bar{S}_n'(x)$ respectively.

We shall transform the series $\mathfrak{T}$ by a regular matrix a_{mn}. This transform is given by

$$T_m(x, F) \sim \sum_{n=0}^{\infty} a_{mn} A_n(x) . \tag{17}$$

We do not require that the series (17) converge but we do require that it be a Fourier series (Cf. Hille and Tamarkin [6]). The series (17) will be a Fourier series if there exists a kernel $K(t, \mathfrak{T})$ which is either, integrable, over $(-\pi, \pi)$ or $(-\infty, \infty)$, or odd and of bounded variation over $(-\infty, \infty)$, and such that,

$$\sum_{n=0}^{\infty} a_{mn} A_n(x) \sim \int_{-\pi}^{\pi} f(x + t) K_m(t, \mathfrak{T}) \, dt$$

or

$$\sum_{n=0}^{\infty} a_{mn}A_n(x) \sim \int_{-\infty}^{\infty} f(x+t)K_m(t, \mathfrak{T})\,dt.$$

The methods of summation considered in the sequel are of one of these types.

Let E_F be a point set in the interval $(-\pi, \pi)$ such that at every point $x \subset E_F$, $F(x)$ has a definite value and satisfies prescribed regularity conditions. We now state our three principal definitions (Cf. Hille and Tamarkin [5, §2]).

Definition 1. A method of summation is said to be *$(\mathfrak{T}, E)$-effective* if, whenever $F(x) \subset \mathfrak{T}$, the series (17) is a Fourier series and

$$T_m(x, F) \to F(x) \text{ as } m \to \infty, \text{ if } x \subset E_F. \tag{18}$$

Definition 2. A point x at which $f(x)$ has a definite value is said to be:
(i) *(F)-regular* if $\varphi(t) \to 0$ as $t \to 0$ (written $x \subset E(F, f)$);
(ii) *(L)-regular* if $\Phi(t) = o(t)$ as $t \to 0$ (written $x \subset E(L, f)$);
(iii) *$(\tilde{F})$-regular* if $\tilde{f}(x)$ exists and is finite and $\psi(t) \to 0$ as $t \to 0$ (written $x \subset E(\tilde{F}, f)$);
(iv) *$(\tilde{L})$-regular* if $\tilde{f}(x)$ exists and is finite and $\Psi(t) = o(t)$ as $t \to 0$ (written $x \subset E(\tilde{L}, f)$);
(v) *(L')-regular* if $f(x)$ is of bounded variation on $(-\pi, \pi)$, $f'(x)$ exists and is finite and $\chi_0(t) = o(t)$ as $t \to 0$ (written $x \subset E(L', f)$);
(vi) *$(\tilde{L}')$-regular* if $f(x)$ is of bounded variation on $(-\pi, \pi)$, $\tilde{f}'(x)$ exists and is finite and $\varphi_0(t) = o(t)$ as $t \to 0$ (written $x \subset E(\tilde{L}', f)$).

Definition 3. A method of summation which is $(\mathfrak{T}, E_F)$-effective is said to be:
(i) *(F)-effective* if $\mathfrak{T} = L$, $E_F = E(F, f)$;
(ii) *(L)-effective* if $\mathfrak{T} = L$, $E_F = E(L, f)$;
(iii) *$(\tilde{F})$-effective* if $\mathfrak{T} = \tilde{L}$, $E_F = E(\tilde{F}, f)$;
(iv) *$(\tilde{L})$-effective* if $\mathfrak{T} = \tilde{L}$, $E_F = E(\tilde{L}, f)$;
(v) *(L')-effective* if $\mathfrak{T} = L'$, $E_F = E(L', f)$;
(vi) *$(\tilde{L}')$-effective* if $\mathfrak{T} = \tilde{L}'$, $E_F = E(\tilde{L}', f)$.

The first note contains an example of a method of summation which is $(\tilde{F})$-effective but not $(\tilde{L})$-effective. This method is similar to one defined by Paley, Randels and Rosskopf [7] which is (F)-effective but not (L)-effective.

In the second note a method of summation is defined which is both (L)-effective and $(\tilde{L})$-effective but neither (L')-effective nor $(\tilde{L}')$-effective.

Hardy and Littlewood [4] have recently shown that, if $\int_{-\pi}^{\pi} \varphi(t)\,dt = 0$, sufficient conditions for the convergence of the Fourier series of $f(x)$ at $x = 0$ are,

$$\Phi(t) = o(t/\log 1/t) \text{ as } t \to 0, \tag{19}$$

and either

$$a_n = O(n^{-\gamma}), \text{ for some } \gamma > 0, \tag{20}$$

or

$$(21) \qquad \varphi_\Delta(t) = \int_0^t |\, du^\Delta \varphi(u) \,| = O(t), \text{ for some } \Delta < \infty.$$

They mention that they have been unable to replace the condition (19) by

$$(22) \qquad \varphi_1(t) = o(t/\log 1/t) \text{ as } t \to 0 .$$

In the third note we show that, given any $\gamma < 1$, any $\Delta > 1$ and any function $\alpha(t)$ such that

$$(23) \qquad \alpha(t) \downarrow 0 \text{ as } t \to 0, \qquad \alpha(t)t^{-\beta} \to \infty \text{ as } t \to 0, \text{ for every } \beta > 0,$$

we can construct a function $f(x)$ which satisfies the conditions (20) and (21) for the given γ and Δ and for which at $x = 0$,

$$(24) \qquad \varphi_1(t) = o(t\alpha(t)),$$

but such that the Fourier series of $f(x)$ does not converge at $x = 0$. It is clear that the function $\alpha(t) = (\log 1/t)^{-1}$ satisfies (23). The method of attack on this problem was suggested by a proof of Hahn [2] that the condition

$$\varphi_1(t) = o(t) \text{ as } t \to 0$$

is not sufficient for the $(C, 1)$ summability of the Fourier series of $f(x)$.

I. A Method of Summation which is $(\bar{F})$-effective but not $(\bar{L})$-effective

2. We shall consider a method of summation for which $a_{mn} = a(n/m)$. The function $a(x)$ need only be defined for rational x but it is more convenient to consider it as defined everywhere on the interval $(0, \infty)$. It can be easily shown that necessary and sufficient conditions that such a method be regular are:

$$(1.01) \qquad a(0) = a(+0) = 1,$$

$$(1.02) \qquad a(x) \subset B.V. \text{ over } (0, \infty).$$

If in addition we impose the condition,

$$(1.03) \qquad a(x) \to 0, \text{ as } x \to \infty,$$

we know from the theory of the Fourier integral[2] that the function

$$(1.04) \qquad K(t) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_0^\infty a(x) \sin xt \, dx$$

[2] See Bochner [1, Theorem 1].

will exist for all t. Conversely, under suitable restrictions on $a(x)$ or $K(t)$, $a(x)$ will be given by

$$(1.05) \qquad a(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_0^\infty K(t) \sin xt \, dt.$$

In particular, if $a(x)$ is continuous and $a(x)/x$ is integrable for large values of x, the inversion is possible.[3] Consequently we may think of the method of summation as determined by the kernel $K(t)$.

We propose to find a kernel $K(t)$ which defines an $(\tilde{F})$-effective method of summation (K) and an odd function $f(x)$ of period 2π such that the point $x = 0$ is $(\tilde{L})$-regular but such that its conjugate Fourier series is not summable (K) at $x = 0$.

3. We define $K(t)$ as follows:

$$K(t) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \begin{cases} 1, & 0 \leqq t \leqq 1, \\ 1/t + \dfrac{(-1)^n}{tn^{\frac{1}{2}}} (n^{\frac{1}{2}} - 2 \mid t - 2^n \mid), & \mid t - 2^n \mid \leqq \frac{1}{2} n^{\frac{1}{2}} \quad (n = 1, 2 \cdots), \\ 1/t, & \text{elsewhere on } (0, \infty). \end{cases}$$

This kernel has the properties:

$$(1.06) \qquad K(t)/t \subset L, \text{ over } (x, \infty), x > 0;$$

$$(1.07) \qquad K(t) \subset B.V., \text{ over } (0, \infty).$$

If $K_1(t) = K(t) - (2/\pi)^{\frac{1}{2}} 1/t$,

$$(1.08) \qquad K_1(t) \subset L, \text{ over } (x, \infty), x > 0;$$

$$(1.09) \qquad K_1(t) \subset B.V., \text{ over } (x, \infty), x > 0;$$

$$(1.10) \qquad \int_t^\infty \mid dK_1(\tau) \mid = O\left(\sum_{n=[\log_2 t]}^{\infty} 2^{-n} n^{-1} \right) = o(1/t) \text{ as } t \to \infty;$$

$$(1.11) \qquad tK_1(t) \subset L_2, \text{ over } (0, \infty).$$

By the Plancherel theorem and (1.11)

$$(1.12) \qquad a_1'(x) \equiv \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_0^\infty tK_1(t) \cos xt \, dt \subset L_2 \text{ over } (0, \infty),$$

where the integral is considered as a limit in the mean. If we set $\delta_n = 2^n - \dfrac{n^{\frac{1}{2}}}{2}$, $\epsilon_n = 2^n + \dfrac{n^{\frac{1}{2}}}{2}$, then almost everywhere,

[3] For more general conditions see Bochner [1, Theorem 11a].

$$
\begin{aligned}
a_1'(x) &= \frac{2}{\pi}\int_0^1 (t-1)\cos xt\,dt + \sum_{n=1}^{\infty}\frac{2}{\pi}(-1)^n n^{-\frac12} \int_{\delta_n}^{\epsilon_n} (n^{\frac12} - 2\,|\,t - 2^n\,|)\cos xt\,dt \\
&= \frac{2}{\pi}\,\frac{\cos x - 1}{x^2} + \frac{2}{\pi}\sum_{n=1}^{\infty}\frac{2(-1)^n}{xn^{\frac12}}\left\{-\int_{\delta_n}^{2^n}\sin xt\,dt + \int_{2^n}^{\epsilon_n}\sin xt\,dt\right\} \qquad (1.13)\\
&= \frac{2}{\pi}\,\frac{\cos x - 1}{x^2} + \frac{2}{\pi}\sum_{n=1}^{\infty}\frac{4(-1)^n}{x^2 n^{\frac12}}\left(1 - \cos\frac{1}{2}n^{\frac12}x\right)\cos 2^n x .
\end{aligned}
$$

Therefore

$$a_1'(x) \subset L \text{ over } (0,\ \infty).$$

Since the series (1.13) converges uniformly over $(\epsilon,\ \infty)$, for every $\epsilon > 0$, we have

$$
\begin{aligned}
a_1(x) &\equiv \int_0^x a_1'(u)\,du = \lim_{\epsilon\to 0}\int_\epsilon^x a_1'(u)\,du \\
&= \lim_{\epsilon\to 0}\left\{\frac{2}{\pi}\int_\epsilon^x \frac{\cos u - 1}{u^2}\,du + \frac{2}{\pi}\sum_{n=1}^{\infty}\int_\epsilon^x \frac{4(-1)^n}{u^2 n^{\frac12}}\left(1 - \cos\frac{1}{2}n^{\frac12}u\right)\cos 2^n u\,du\right\} \\
&= \left(\frac{2}{\pi}\right)^{\frac12}\int_0^\infty K_1(t)\sin xt\,dt .
\end{aligned}
$$

This shows that the sine Fourier transform of $K_1(t)$ is absolutely continuous on $(0,\ \infty)$. Since the sine Fourier transform of $(2/\pi)^{\frac12}\,1/t$ is identically 1, it is also absolutely continuous. Therefore

$$a(x) = \left(\frac{2}{\pi}\right)^{\frac12}\int_0^\infty K(t)\sin xt\,dt \subset \text{B. V. over } (0,\ \infty). \tag{1.14}$$

Since $a_1'(x) \subset L$ over $(0,\ \infty)$, $a_1(x) \to 0$ as $x \to 0$ and $a(0) = 1$. Since $K(t) \subset B.V.$ over $(0,\ \infty)$, $a(x) \to 0$ as $x \to \infty$. Therefore conditions (1.01)–(1.03) are satisfied. Moreover since $K(t)$ is continuous and satisfies (1.06) and (1.07), by a previous remark

$$K(t) = \left(\frac{2}{\pi}\right)^{\frac12}\int_0^\infty a(x)\sin xt\,dt .$$

4. To prove that the method (K) is $(\tilde{F})$-effective we observe that, if

$$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n\cos nx + b_n\sin nx),$$

then for a given value of x the series

$$\sum_{n=1}^{\infty}(a_n\sin nx - b_n\cos nx)$$

is the same as

$$\frac{1}{2}\sum_{n=1}^{\infty} - b_n(\psi) \tag{1.15}$$

where

$$b_n(\psi) \equiv \frac{1}{\pi}\int_{-\pi}^{\pi} \psi(t) \sin nt\, dt . \tag{1.16}$$

We define the function $\psi_\delta(t)$ by:

$$\psi_\delta(t) = \begin{cases} \psi(t), & |t| \leqq \delta, \\ 0, & \text{elsewhere on } (-\pi, \pi), \\ \psi_\delta(t + 2\pi), & -\infty < t < \infty . \end{cases} \tag{1.17}$$

If $x \subset E(\tilde{F}, f)$, $\psi(t) \to 0$ as $t \to 0$ and it is possible to choose δ so that $\psi_\delta(t)$ is bounded. If $\tilde{f}(x)$ exists and is finite then

$$\tilde{f}_\delta(x) = \lim_{\epsilon \to 0} -\frac{1}{\pi}\int_{\epsilon}^{\infty} \psi_\delta(t)\,\frac{dt}{t}$$

is also finite. Also

$$\psi_\delta(t) \sim \sum_{n=1}^{\infty} b_n(\psi_\delta) \sin nt .$$

We define

$$\tilde{S}_n^\delta(x) = -\frac{1}{2}\sum_{\nu=1}^{n} b_\nu(\psi_\delta) , \tag{1.18}$$

and it is well known that

$$\tilde{S}_n(x) - \tilde{f}(x) - [\tilde{S}_n^\delta(x) - \tilde{f}_\delta(x)] = o(1) \qquad \text{as} \qquad n \to \infty . \tag{1.19}$$

Therefore since the method (K) is regular we need only discuss the summability of the series $-\frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)$. Since $K(t) \subset B.V.$ over $(0, \infty)$,

$$\begin{aligned} \frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta) a\,(n/m) &= \frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)\left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^{\infty} K(t) \sin \frac{nt}{m}\, dt \\ &= \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^{\infty} \frac{1}{2}\psi_\delta(t/m)\, K(t)\, dt , \end{aligned} \tag{1.20}$$

where the termwise integration is justified by a theorem of Hardy [3]. Hence

$$\begin{aligned}(1.21)\quad \frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)a(n/m) &= \frac{1}{\pi}\int_0^1 \psi_\delta(t/m)\,dt + \frac{1}{\pi}\int_1^\infty \psi_\delta(t/m)\frac{dt}{t}\\ &+ \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_1^\infty \frac{1}{2}\psi_\delta(t/m)K_1(t)\,dt = I_1 + I_2 + I_3.\end{aligned}$$

But $I_2 \to -\tilde{f}_\delta(x)$ as $m \to \infty$, and in I_1 and I_3, since $\psi_\delta(t)$ is bounded, the integrand is dominated by an integrable function and tends to zero as $m \to \infty$ for every t, if $x \subset E(\tilde{F}, f)$. Therefore by the Lebesgue theorem $I_1, I_3 = o(1)$ as $m \to \infty$, and

$$(1.22)\quad -\frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)a(n/m) = \tilde{f}_\delta(x) + o(1) \quad \text{as} \quad m \to \infty, \quad \text{if} \quad x \subset E(\tilde{F}, f).$$

This proves that the method (K) is $(\tilde{F})$-effective.

5. We define $f(x)$ by:

$$(1.23)\quad f(x) = \begin{cases} (-1)^n 4^n t, & |t - 2^{-n}| \leqq 4^{-n}/2\log n \qquad (n = 2, 3 \cdots),\\ 0, & \text{elsewhere on} \quad (0, \pi),\\ -f(-x), & -\infty < x < \infty,\\ f(x + 2\pi), & -\infty < x < \infty. \end{cases}$$

Then at $x = 0$, $\psi(t) = 2f(t)$, and

$$(1.24)\quad \int_0^t |\psi(t)|\,dt \leqq 2\sum_{n=[\log_2 1/t]}^{\infty} \frac{2^{-n}}{\log n} = o(2^{-[\log_2 1/t]}) = o(t) \quad \text{as} \quad t \to 0.$$

We define

$$F(t) \equiv \int_\pi^t \psi(t)\,dt = O(1),$$

then

$$\frac{1}{\pi}\int_\pi^\infty \psi(t)\frac{dt}{t} = \frac{1}{\pi}\int_\pi^\infty F(t)\frac{dt}{t^2}$$

is finite. Also

$$\lim_{\epsilon\to 0}\frac{1}{\pi}\int_\epsilon^\pi \psi(t)\frac{dt}{t} = \lim_{\epsilon\to 0}\left(\frac{1}{\pi}\sum_{n=2}^{[\log_2 1/\epsilon]}\frac{2(-1)^n}{\log n} + o(1)\right)$$

is the same as

$$\frac{1}{2}\sum_{n=1}^{\infty} - b_n(\psi) \tag{1.15}$$

where

$$b_n(\psi) \equiv \frac{1}{\pi}\int_{-\pi}^{\pi} \psi(t) \sin nt \, dt . \tag{1.16}$$

We define the function $\psi_\delta(t)$ by:

$$\psi_\delta(t) = \begin{cases} \psi(t), & |t| \leqq \delta, \\ 0, & \text{elsewhere on } (-\pi, \pi), \\ \psi_\delta(t + 2\pi), & -\infty < t < \infty . \end{cases} \tag{1.17}$$

If $x \subset E(\bar{F}, f)$, $\psi(t) \to 0$ as $t \to 0$ and it is possible to choose δ so that $\psi_\delta(t)$ is bounded. If $\bar{f}(x)$ exists and is finite then

$$\bar{f}_\delta(x) = \lim_{\epsilon \to 0} -\frac{1}{\pi}\int_{\epsilon}^{\infty} \psi_\delta(t)\frac{dt}{t}$$

is also finite. Also

$$\psi_\delta(t) \sim \sum_{n=1}^{\infty} b_n(\psi_\delta) \sin nt .$$

We define

$$\tilde{S}_n^\delta(x) = -\frac{1}{2}\sum_{\nu=1}^{n} b_\nu(\psi_\delta) , \tag{1.18}$$

and it is well known that

$$\tilde{S}_n(x) - \bar{f}(x) - [\tilde{S}_n^\delta(x) - \bar{f}_\delta(x)] = o(1) \quad \text{as} \quad n \to \infty . \tag{1.19}$$

Therefore since the method (K) is regular we need only discuss the summability of the series $-\frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)$. Since $K(t) \subset B.V.$ over $(0, \infty)$,

$$\begin{aligned} \frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta) a\,(n/m) &= \frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)\left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^{\infty} K(t) \sin \frac{nt}{m}\, dt \\ &= \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^{\infty} \frac{1}{2}\psi_\delta(t/m)\, K(t)\, dt , \end{aligned} \tag{1.20}$$

where the termwise integration is justified by a theorem of Hardy [3]. Hence

$$\tag{1.21} \begin{aligned} \frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)a(n/m) &= \frac{1}{\pi}\int_0^1 \psi_\delta(t/m)\,dt + \frac{1}{\pi}\int_1^\infty \psi_\delta(t/m)\,\frac{dt}{t} \\ &\quad + \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_1^\infty \frac{1}{2}\psi_\delta(t/m)K_1(t)\,dt = I_1 + I_2 + I_3. \end{aligned}$$

But $I_2 \to -\tilde{f}_\delta(x)$ as $m \to \infty$, and in I_1 and I_3, since $\psi_\delta(t)$ is bounded, the integrand is dominated by an integrable function and tends to zero as $m \to \infty$ for every t, if $x \subset E(\tilde{F}, f)$. Therefore by the Lebesgue theorem $I_1, I_3 = o(1)$ as $m \to \infty$, and

$$\tag{1.22} -\frac{1}{2}\sum_{n=1}^{\infty} b_n(\psi_\delta)a(n/m) = \tilde{f}_\delta(x) + o(1) \quad \text{as} \quad m \to \infty, \quad \text{if} \quad x \subset E(\tilde{F}, f).$$

This proves that the method (K) is $(\tilde{F})$-effective.

5. We define $f(x)$ by:

$$\tag{1.23} f(x) = \begin{cases} (-1)^n 4^n t, & |\,t - 2^{-n}\,| \leqq 4^{-n}/2\log n \qquad (n = 2, 3 \cdots), \\ 0, & \text{elsewhere on} \quad (0, \pi), \\ -f(-x), & -\infty < x < \infty, \\ f(x + 2\pi), & -\infty < x < \infty. \end{cases}$$

Then at $x = 0$, $\psi(t) = 2f(t)$, and

$$\tag{1.24} \int_0^t |\,\psi(t)\,|\,dt \leqq 2 \sum_{n=[\log_2 1/t]}^{\infty} \frac{2^{-n}}{\log n} = o(2^{-[\log_2 1/t]}) = o(t) \quad \text{as} \quad t \to 0.$$

We define

$$F(t) \equiv \int_\pi^t \psi(t)\,dt = O(1),$$

then

$$\frac{1}{\pi}\int_\pi^\infty \psi(t)\,\frac{dt}{t} = \frac{1}{\pi}\int_\pi^\infty F(t)\,\frac{dt}{t^2}$$

is finite. Also

$$\lim_{\epsilon \to 0} \frac{1}{\pi}\int_\epsilon^\pi \psi(t)\,\frac{dt}{t} = \lim_{\epsilon \to 0}\left(\frac{1}{\pi}\sum_{n=2}^{[\log_2 1/\epsilon]} \frac{2(-1)^n}{\log n} + o(1)\right)$$

exists since $\sum_{n=2}^{\infty}(-1)^n/\log n$ converges. Therefore

$$\bar{f}(0) = \lim_{\epsilon\to 0} -\frac{1}{\pi}\int_{\epsilon}^{\infty}\psi(t)\,\frac{dt}{t} \tag{1.25}$$

exists and is finite. From (1.24), (1.25) we see that the point $x = 0$ is $(\bar{L})$-regular.

We propose to show that

$$-\sum_{n=1}^{\infty} b_n(f)a(n/m) - \bar{f}(0) \neq o(1) \qquad \text{as} \qquad m \to \infty. \tag{1.26}$$

As before

$$\begin{aligned}\sum_{n=1}^{\infty} b_n a(n/m) &= \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^{\infty} f(t/m)K(t)\,dt \\ &= \frac{2}{\pi}\int_0^1 f(t/m)\,dt + \frac{2}{\pi}\int_1^{\infty} f(t/m)\,\frac{dt}{t} + \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_1^{\infty} f(t/m)K_1(t)\,dt \\ &= I_1 + I_2 + I_3.\end{aligned} \tag{1.27}$$

But

$$I_2 = -\bar{f}(0) + o(1) \qquad \text{as} \qquad m \to \infty,$$

and

$$I_1 = m\int_0^{1/m} f(t)\,dt = o(1) \qquad \text{as} \qquad m\to\infty$$

so that it is only necessary to consider I_3. We have

$$I_3 = \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_1^{m} f(t/m)K_1(t)\,dt + \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_m^{\infty} f(t/m)K_1(t)\,dt = I_3' + I_3''.$$

If we define

$$G(t) \equiv \int_m^t f(t/m)\,dt = m\int_1^{t/m} f(t)\,dt = O(m), \tag{1.28}$$

we have by (1.10)

$$I_3'' = -\int_m^{\infty} G(t)\,dK_1(t) = O\left(m\int_m^{\infty} |\,dK_1(t)\,|\right) = o(1) \quad \text{as} \quad m\to\infty. \tag{1.29}$$

We choose $m = 2^h$, h even. Then

$$f(t2^{-h}) = \begin{cases} (-1)4^n t 2^{-h}, & |\,t - 2^{h-n}\,| \leq \dfrac{4^{-n}2^h}{2\log n}\ (n = 2, 3, \cdots), \\ 0, & \text{elsewhere on} \quad (0, 2^h). \end{cases} \tag{1.30}$$

We have on the interval $(1, 2^h)$, $f(t2^{-h})K(t) \geqq 0$. Since, for h sufficiently large,

$$\frac{4^{-n}2^h}{2\log n} \leqq \frac{1}{2\log n} < \frac{1}{4}(h-n)^{\frac{1}{2}}, \qquad h > n \geqq \frac{h}{2},$$

on the interval

$$J_n = \left(2^{-n+h} - \frac{4^{-n}2^h}{2\log n}, \qquad 2^{-n+h} + \frac{4^{-n}2^h}{2\log n}\right), \qquad h > n \geqq \frac{h}{2},$$

we must have, for such h,

$$tK_1(t) > \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \frac{1}{2(h-n)}.$$

Hence

$$I_3' = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_1^{2^h} f(t2^{-h})K_1(t)\, dt > \sum_{n=h/2}^{h-1} \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_{J_n} f(t2^{-h})K_1(t)\, dt$$

$$> \frac{1}{2} \sum_{n=h/2}^{h-1} \frac{2}{\pi(h-n)\log n} > \frac{1}{\pi \log h} \sum_{n=1}^{h/2} n^{-1} \sim \frac{1}{\pi}.$$

Therefore I_3' does not tend to zero and hence the conjugate Fourier series of $f(x)$ is not summable (K) at $x = 0$ to $\bar{f}(0)$, which implies that the method (K) is not $(\bar{L})$-effective.

II. A Method of Summation which is (L)-effective and $(\bar{L})$-effective but not (L')-effective or $(\bar{L}')$-effective.

6. A Woronoï-Nörlund method of summation is defined by a sequence $p_n (n = 0, 1, \cdots)$, the related sequence $P_n = \sum_{\nu=0}^{n} p_\nu$, and the transformation

$$T_m(x, F) = \frac{1}{P_m} \sum_{n=0}^{m} F_n(x) p_{m-n}. \tag{2.01}$$

Necessary and sufficient conditions for the regularity of such a method are:[4]

$$\sum_{n=0}^{m} |p_n| < CP_m, \qquad \frac{p_n}{P_n} \to 0 \text{ as } n \to \infty. \tag{2.02}$$

The method we shall consider is defined by:[5]

$$p_n = \begin{cases} 1, & n \equiv 0 \pmod 4, \\ 0, & \text{otherwise.} \end{cases} \tag{2.03}$$

We denote this method by (N, p_n). It is clearly regular.

[4] See e.g. Hille and Tamarkin [5, (1.05)].

[5] This method differs from those considered by Hille and Tamarkin [5] in that their condition (3.02) is not satisfied.

We prove first that our method (N, p_n) is (L)-effective. We use the familiar formula

$$S_n(x) - f(x) = \int_0^\pi \varphi(t) \frac{\sin (n + \frac{1}{2}) t}{2\pi \sin t/2} \, dt. \tag{2.04}$$

Then, if $\sigma_m(x) = 1/P_m \sum_{n=0}^{m} S_n(x) p_{m-n}$,

$$\sigma_m(x) - f(x) = \int_0^\pi \varphi(t) K_m(t) \, dt, \tag{2.05}$$

where, if $m \equiv a \pmod 4$,

$$K_m(t) = \frac{1}{P_m} \sum_{n=0}^{m} \frac{\sin (n + \frac{1}{2}) t}{2\pi \sin t/2} p_{m-n} = \frac{1}{P_m} \sum_{n=0}^{[m/4]} \frac{\sin (4n + a + \frac{1}{2}) t}{2\pi \sin t/2}, \tag{2.06}$$

and, since

$$\sin (4n + a + \tfrac{1}{2})t \sin 2t = \tfrac{1}{2}\{\cos (4n + a - 2 + \tfrac{1}{2})t - \cos (4n + a + 2 + \tfrac{1}{2})t\},$$

we have

$$\begin{aligned} K_m(t) &= \frac{1}{4\pi P_m \sin t/2 \sin 2t} \{\cos (a - 2 + \tfrac{1}{2}) t - \cos (m + 2 + \tfrac{1}{2}) t\} \\ &= O\left(\frac{1}{mt^2}\right), \quad \text{if } |t| < \frac{\pi}{4}. \end{aligned} \tag{2.07}$$

Moreover, since $\sin (n + \frac{1}{2})t/2\pi \sin t/2 = O(n)$, we have

$$K_m(t) = O(m) \text{ uniformly in } t. \tag{2.08}$$

Now

$$\sigma_m(x) - f(x) = \int_0^{1/m} \varphi(t) K_m(t) \, dt + \int_{1/m}^{\delta} \varphi(t) K_m(t) \, dt + \int_\delta^\pi \varphi(t) K_m(t) \, dt$$

$$= I_1 + I_2 + I_3,$$

and

$$I_1 = O\left(m \int_0^{1/m} |\varphi(t)| \, dt\right) = o(1) \text{ as } m \to \infty \text{ if } x \subset E(L, f),$$

$$I_2 = O\left(\int_{1/m}^{\delta} |\varphi(t)| \frac{dt}{mt^2}\right) = O\left(\frac{\Phi(t)}{mt^2}\bigg|_{1/m}^{\delta} + \int_{1/m}^{\delta} \Phi(t) \frac{dt}{mt^3}\right) = o(1)$$

uniformly in m as $\delta \to 0$, if $x \subset E(L, f)$. Finally, by the Riemann-Lebesgue theorem, for a fixed δ,

$$\int_\delta^\pi \varphi(t) \frac{\sin (n + \frac{1}{2}) t}{2\pi \sin t/2} \, dt = o(1) \text{ as } n \to \infty,$$

and therefore, since the method (N, p_n) is regular, for a fixed δ

$$I_3 = \int_\delta^\pi \varphi(t)K_m(t)\, dt = o(1) \text{ as } m \to \infty.$$

From this it results that

$$\int_0^\pi \varphi(t)K_m(t)\, dt = o(1) \text{ as } m \to \infty \tag{2.09}$$

and the method (N, p_n) is shown to be (L)-effective.

7. We now prove that our method (N, p_n) is $(\bar{L})$-effective. We use the formula

$$\tilde{S}_n(x) = \frac{1}{2\pi}\int_0^\pi \psi(t)\left\{-\cot t/2 + \frac{\cos(n+\frac{1}{2})t}{\sin t/2}\right\} dt. \tag{2.10}$$

Then

$$\tilde{\sigma}_m(x) = \frac{1}{P_m}\sum_{n=0}^m \tilde{S}_n(x)p_{m-n} = \int_0^\pi \psi(t)\left\{-\frac{1}{2\pi}\cot t/2 + \tilde{K}_m(t)\right\} dt, \tag{2.11}$$

where, if $m \equiv a (\text{mod } 4)$,

$$\tilde{K}_m(t) = \frac{1}{P_m}\sum_{n=0}^m \frac{\cos(n+\frac{1}{2})t}{2\pi \sin t/2} p_{m-n} = \frac{1}{P_m}\sum_{n=0}^{[m/4]} \frac{\cos(4n+a+\frac{1}{2})t}{2\pi\sin t/2}. \tag{2.12}$$

Since

$$\cos(4n+a+\tfrac{1}{2})t \sin 2t = \tfrac{1}{2}\{\sin(4n+a+2+\tfrac{1}{2})t - \sin(4n+a-2+\tfrac{1}{2})t\}$$

we have

$$\begin{aligned}\tilde{K}_m(t) &= \frac{1}{4\pi P_m \sin 2t \sin t/2}\{\sin(m+2+\tfrac{1}{2})t - \sin(a-2+\tfrac{1}{2})t\}\\ &= O\left(\frac{1}{mt^2}\right), \text{ if } |t| < \frac{\pi}{4}.\end{aligned} \tag{2.13}$$

From (2.11)

$$\begin{aligned}\tilde{\sigma}_m(x) &= \int_0^{1/m} \psi(t)\left\{-\frac{1}{2\pi}\cot t/2 + \tilde{K}_m(t)\right\} dt + \int_{1/m}^\pi \psi(t)\tilde{K}_m(t)\, dt\\ &\quad - \frac{1}{2\pi}\int_{1/m}^\pi \psi(t)\cot t/2\, dt = I_1 + I_2 + I_3.\end{aligned}$$

From the definition of $\tilde{f}(x)$, $I_3 \to \tilde{f}(x)$ as $m \to \infty$. We know that

$$\frac{1}{2\pi}\left\{-\cot t/2 + \frac{\cos(n+\frac{1}{2})t}{\sin t/2}\right\} = O(n) \text{ uniformly in } t,$$

and consequently

$$-\frac{1}{2\pi}\cot t/2 + \tilde{K}_m(t) = O(m) \text{ uniformly in } t.$$

Hence

$$I_1 = O\left(m\int_0^{1/m} |\psi(t)|\,dt\right) = o(1) \text{ as } m \to \infty, \text{ if } x \subset E(\tilde{L}, f).$$

We set

$$I_2 = \int_{1/m}^{\delta} \psi(t)\tilde{K}_m(t)\,dt + \int_{\delta}^{\pi} \psi(t)\tilde{K}_m(t)\,dt = I_2' + I_2''.$$

Then using (2.13)

$$I_2' = O\left(\int_{1/m}^{\delta} |\psi(t)| \frac{dt}{mt^2}\right) = O\left(\frac{\Psi(t)}{mt^2}\bigg|_{1/m}^{\delta} + \int_{1/m}^{\delta} \Psi(t)\frac{dt}{mt^3}\right)$$
$$= o(1) \text{ uniformly in } m \text{ as } \delta \to 0, \text{ if } x \subset E(\tilde{L}, f).$$

Moreover, by the Riemann-Lebesgue theorem, for a fixed δ,

$$\int_{\delta}^{\pi} \psi(t)\frac{\cos(n+\frac{1}{2})t}{2\pi \sin t/2}\,dt = o(1) \text{ as } n \to \infty,$$

and therefore, for a fixed δ,

$$I_2'' = o(1) \text{ as } m \to \infty.$$

From this it results that

$$I_2 = o(1) \text{ as } m \to \infty,$$

and hence

$$\tilde{\sigma}_m(x) = \tilde{f}(x) + o(1) \text{ as } m \to \infty.$$

Therefore the method (N, p) is $(\tilde{L})$-effective.

8. However the method (N, p_n) is not (L')-effective. Indeed consider the function:

$$f(x) = \begin{cases} 0, & |x| \leqq \frac{\pi}{2}, \quad x = \pi, \\ \operatorname{sgn} x, & \frac{\pi}{2} < |x| < \pi, \\ f(x+2\pi), & -\infty < x < \infty. \end{cases}$$

For this function $f'(0) = 0$, and $\chi(t) = 2f(t)$ at $x = 0$. Hence $\chi_0(t) = 0$, if $|t| < \pi/2$, and the point $x = 0$ is (L')-regular. Also $a_n = 0$,

$$b_n = \frac{2}{n\pi}\begin{cases} 0, & n \equiv 0 \pmod 4, \\ 1, & n \equiv 1 \pmod 4, \\ -2, & n \equiv 2 \pmod 4, \\ 1, & n \equiv 3 \pmod 4, \end{cases}$$

and

$$S_n'(0) = \frac{2}{\pi}\begin{cases} 0, & n \equiv 0 \pmod 4, \\ 1, & n \equiv 1 \pmod 4, \\ -1, & n = 2 \pmod 4, \\ 0, & n \equiv 3 \pmod 4. \end{cases}$$

If $m \equiv 1 \pmod 4$

$$\sigma_m'(0) = \frac{1}{P_m}\sum_{n=0}^{[m/4]} S_{4n+1}'(0) = \frac{2}{\pi}$$

and hence $\sigma_m'(0)$ cannot tend to $f'(0)$ as $m \to \infty$.

Finally we show that the method (N, p_n) is not $(\tilde{L}')$-effective. We consider the function:

$$f(x) = \begin{cases} 0, & |x| \leqq \frac{\pi}{2}, \\ 1, & \frac{\pi}{2} < |x| \leqq \pi \\ f(x + 2\pi), & -\infty < x < \infty. \end{cases}$$

At $x = 0$, $\varphi(t) = 2f(t)$. Consequently $\varphi_0(t) = 0$, if $|t| < \pi/2$ and,

$$\tilde{f}'(0) = -\frac{1}{2\pi}\int_0^\pi f(t)(\sin t/2)^{-2}\,dt = -\frac{1}{2\pi}\int_{\pi/2}^\pi (\sin t/2)^{-2}\,dt \neq 0,$$

is finite. Therefore the point $x = 0$ is $(\tilde{L}')$-regular. Also $b_n = 0$, $a_0 = 1$ and

$$a_n = \frac{2}{n\pi}\begin{cases} 0, & n \equiv 0 \pmod 4, \quad n \neq 0, \\ -1, & n \equiv 1 \pmod 4, \\ 0, & n \equiv 2 \pmod 4, \\ 1, & n \equiv 3 \pmod 4. \end{cases}$$

Therefore

$$\tilde{S}_n'(0) = \frac{2}{\pi}\begin{cases} 0, & n \equiv 0 \pmod 4, \\ -1, & n \equiv 1 \pmod 4, \\ -1, & n \equiv 2 \pmod 4, \\ 0, & n \equiv 3 \pmod 4. \end{cases}$$

If $m \equiv 0 \pmod 4$

$$\tilde{\sigma}'_m(0) = \frac{1}{P_m} \sum_{n=0}^{[m/4]} S'_{4n}(0) = 0 .$$

Therefore $\tilde{\sigma}'_m(0)$ cannot tend to $\tilde{f}'(0)$ and the method (N, p_n) is not $(\tilde{L}')$-effective.

III. On Two Theorems of Hardy and Littlewood

9. As mentioned in the introduction we have given that $\gamma < 1$, $\Delta > 1$ and

$$\text{(3.01)} \qquad \alpha(t) \downarrow 0 \text{ as } t \to 0, \qquad \alpha(t)t^{-\beta} \to \infty \text{ as } t \to 0, \text{ for every } \beta > 0,$$

and we wish to construct a function $f(x)$ such that at $x = 0$

$$\text{(3.02)} \qquad a_n = O(n^{-\gamma}),$$

$$\text{(3.03)} \qquad \varphi_\Delta(t) = \int_0^t |\, du^\Delta \varphi(u)\,| = O(t),$$

and

$$\text{(3.04)} \qquad \varphi_1(t) = o(t\alpha(t)),$$

but such that the Fourier series of $f(x)$ does not converge at $x = 0$. We may assume without loss of generality that

$$\text{(3.05)} \qquad \alpha(t) = o(1/\log 1/t),$$

for if (3.04) is satisfied for a given function $\alpha(t)$ it will be satisfied for every function which decreases more slowly than $\alpha(t)$.

Let δ be chosen so that $1 < \delta < 2$. We define the set of integers

$$n_1 = 5 \cdots n_i = n_{i-1}[n_{i-1}^{\delta-1} + \eta_i]$$

where $\eta_i = 1$ or 2 is chosen so that $[n_{i-1}^{\delta-1} + \eta_i]$ is odd. These integers have the properties,

$$\text{(3.06)} \qquad n_i > 2^{\delta^i}, \qquad n_i = \epsilon_i n_{i-1}^\delta, \text{ where } \epsilon_i > 1, \text{ and } \epsilon_i \to 1, \text{ as } i \to \infty .$$

We introduce the sequence of points $x_i = \pi/2n_i$. A function $F(x)$ is defined by recursion as follows. Let

$$\text{(3.07)} \qquad F(x) = 0, \qquad x_1 \leqq |x| \leqq \pi;$$

$$\text{(3.08)} \qquad F(x) = d_i x \cos n_i x, \qquad x_i \leqq |x| < x_{i-1},$$

where

$$\text{(3.09)} \qquad d_i = \begin{cases} \alpha^2(x_i), \text{ if } \left| \dfrac{1}{\pi} \displaystyle\int_{x_{i-1}}^{\pi} F'(t) \frac{\sin (n_i + 1/2)t}{\sin t/2} \right| < \Big| \\ 0, \quad \text{otherwise}; \end{cases}$$

$$\text{(3.10)} \qquad F(0) = 0 .$$

It is easily seen from (3.09) and (3.05) that

$$d_i = o\,((\log n_i)^{-2}) = o(\delta^{-2i})$$

and therefore, since $\delta > 1$,

$$\sum_{i=2}^{\infty} d_i \tag{3.11}$$

converges. The function $F(x)$ is continuous, for since x_{i-1} is an odd multiple of $\pi/2n_i$, $\cos n_i x_{i-1} = 0$, and $F(x) \to 0$ as $x \to 0$. It is clear that $F(x)$ is absolutely continuous on every interval (ϵ, π), $\epsilon > 0$. Moreover it is absolutely continuous on $(0, \pi)$ for

$$\begin{aligned}
\int_0^{\pi} | F'(x) | \, dx &= \sum_{i=2}^{\infty} \int_{x_i}^{x_{i-1}} | F'(x) | \, dx \\
&= \sum_{i=2}^{\infty} d_i \int_{x_i}^{x_{i-1}} | - x n_i \sin n_i x + \cos n_i x | \, dx \\
&= O\Big(\sum_{i=2}^{\infty} d_i (x_{i-1}^2 \, n_i + x_{i-1}) \Big) \\
&= O\Big(\sum_{i=2}^{\infty} d_i (n_{i-1}^{\delta-2} + n_{i-1}^{-1}) \Big) = O(1).
\end{aligned} \tag{3.12}$$

It should be remarked here that by the Riemann-Lebesgue theorem it can be seen that there will be an infinite number of non-zero d_i. The function $f(x)$ is then defined by,

$$f(x) = \begin{cases} F'(x)\,, & -\pi \leqq x \leqq \pi\,, \quad | x | \neq x_i\,, \\ f(x+0)\,, & x = x_i\,, \\ f(x-0)\,, & x = -x_i\,, \\ f(x+2\pi)\,, & -\infty < x < \infty\,. \end{cases} \tag{3.13}$$

10. To estimate $\varphi_1(t)$ we observe that $f(0) = \lim_{x \to 0} \frac{1}{x} F(x) = 0$ and therefore at $x = 0$,

$$\varphi(t) = 2 f(t)\,, \qquad \varphi_1(t) = 2 F(t)\,. \tag{3.14}$$

Hence

$$\int_{-\pi}^{\pi} \varphi(t) \, dt = 2 F(\pi) - 2 F(-\pi) = 0$$

and

$$| \varphi_1(t) | \leqq 2 d_i t \leqq 2 t \alpha^2(x_i) \qquad x_i \leqq t < x_{i-1}\,.$$

Since $\alpha(t) \downarrow 0$ as $t \to 0$ we have

$$(3.15) \qquad \varphi_1(t) = o(t\alpha(t)) \text{ as } t \to 0 .$$

11. To estimate a_n we define for every n $i_1 = i_1(n)$ as the largest integer such that $n_{i_1} \leqq n/2$, and $i_2 = i_2(n)$ as the smallest integer such that $n_{i_2} \geqq (n/2)^\delta$. It can be seen from (3.06) that $i_2 - i_1 \leqq 2$. We define $j = j(n)$ by $j = i_1 + 1$. Then

$$(3.16) \qquad a_n = \frac{2}{\pi}\int_0^\pi f(x) \cos nx \, dx = \sum_{i=2}^{\infty} \frac{2}{\pi} \int_{x_i}^{x_{i-1}} f(x) \cos nx \, dx .$$

Now

$$(3.17) \qquad \int_{x_j}^{x_{j-1}} f(x) \cos nx \, dx = O\left(d_j \int_{x_j}^{x_{j-1}} (n_j x + 1) \, dx\right)$$

$$= O(d_j x_{j-1}^2 n_j + x_{j-1} d_j) = o(n_j^{1-2/\delta} + n_j^{-1/\delta}) = o(n^{1-2/\delta} + n^{-1/\delta}) .$$

If $n_i \neq n$, we have

$$\int_{x_i}^{x_{i-1}} f(x) \cos nx \, dx = di \int_{x_i}^{x_{i-1}} \{- xn_i \sin n_i x + \cos n_i x\} \cos nx \, dx$$

$$= \frac{d_i}{2} \int_{x_i}^{x_{i-1}} \{xn_i[\sin (n - n_i)x - \sin (n + n_i)x] + \cos (n + n_i)x + \cos (n - n_i)x\} \, dx$$

$$= \frac{d_i}{2}\left[\frac{xn_i \cos (n + n_i)x}{n + n_i} - \frac{xn_i \cos (n - n_i)x}{n - n_i}\right]_{x_i}^{x_{i-1}}$$

$$+ \frac{d_i}{2}\left[\frac{n_i \sin (n - n_i)x}{(n - n_i)^2} - \frac{n_i \sin (n + n_i)x}{(n + n_i)^2}\right]_{x_i}^{x_{i-1}}$$

$$+ \frac{d_i}{2}\left[\frac{\sin (n - n_i)x}{n - n_i} + \frac{\sin (n + n_i)x}{n + n}\right]_{x_i}^{x_{i-1}}$$

$$= H_i(n) + J_i(n) + I_i(n) .$$

If $i \leqq i_1$,

$$\frac{n_i}{n_{i-1}(n \pm n_i)} = O\left(\frac{n_{i-1}^{\delta-1}}{n}\right) = O(n^{\delta-2})$$

and

$$\frac{n_i}{(n \pm n_i)^2} = O\left(\frac{n}{n^2}\right) = (n^{-1}).$$

Therefore, if $i \leqq i_1$,

$$H_i(n) = O(d_i n^{\delta-2}), \qquad J_i(n) = O(d_i n^{-1})$$

and

$$\text{(3.18)} \qquad \sum_{i=2}^{i_1} \{H_i(n) + J_i(n)\} = O\left(n^{\delta-2} \sum_{i=2}^{i_1} d_i\right) = O(n^{\delta-2}).$$

If $i \geqq i_2$ and n is sufficiently large

$$\frac{n_i}{n_{i-1}(n \pm n_i)} = O(n_{i-1}^{-1}) = O(n^{-1})$$

and

$$\frac{n_i}{(n \pm n_i)^2} = O(n_i^{-1} = (On^{-1})$$

so that for $i \geqq i_2$, and n sufficiently large,

$$H_i(n) = O(d_i n^{-1}), \qquad J_i(n) = O(d_i n^{-1})$$

and

$$\text{(3.19)} \quad \sum_{i=i_2}^{\infty} \{H_i(n) + J_i(n)\} = O\left(n^{-1} \sum_{i=i_2}^{\infty} d_i\right) = o(n^{-1})$$

Finally if $i \neq j$ and n is sufficiently large, $| n \pm n_i | \geqq n/2$ and $| I_i(n) | \leqq 2d_i/n$. Hence

$$\text{(3.20)} \qquad \left(\sum_{i=2}^{i_1} = \sum_{1=i_2}^{\infty}\right) I_i(n) = O\left(n^{-1} \sum_{i=2}^{\infty} d_i\right).$$

Combining (3.17)–(3.20) we have

$$\text{(3.21)} \qquad a_n = O(n^{-1} + n^{1-2/\delta} + n^{-1/\delta} + n^{\delta-2}) = O(n^{-\gamma})$$

if $1 < \delta \leqq 2/(\gamma + 1)$.

12. We pass on to the estimation of $\varphi_\Delta(t)$. Since

$$\text{(3.22)} \qquad u^\Delta\varphi(u) = 2d_i u^\Delta\{- un_i \sin n_i u + \cos n_i u\} \quad x_i \leqq u < x_{i-1},$$

$u^\Delta\varphi(u)$ is absolutely continuous on the interior of every interval (x_i, x_{i-1}). Let $S(u)$ be the saltus function of $u^\Delta\varphi(u)$; it will of course have jumps only at the points x_i and

$$\text{(3.23)} \qquad \begin{aligned} J(x_i) \equiv S(x_i + 0) - S(x_1 - 0) &= - 2d_i n_i x^{\Delta+1} \pm 2d_{i+1}n_{i+1}x_i^{\Delta+1} \\ &= O(d_i n_{i+1} n_i^{-\Delta-1}) = O(d_i n_i^{\delta-1-\Delta}). \end{aligned}$$

The function

$$\xi(u) = u^{\Delta}\varphi(u) - S(u)$$

is absolutely continuous on every interval (ϵ, π), $\epsilon > 0$, and, as will be seen, is absolutely continuous on the interval $(0, \pi)$. We have on the interval (x_i, x_{i-1})

$$\begin{aligned} \xi'(u) &= \{u^{\Delta}\varphi(u)\}' \\ &= 2d_i\{- n_i^2 u^{\Delta+1} \cos n_i u - (\Delta + 1)n_i u^{\Delta} \sin n_i u - n_i u^{\Delta} \sin n_i u \\ &\qquad + \Delta u^{\Delta-1} \cos n_i u\} \\ &= O(d_i[n_i^2 x_{i-1}^{\Delta+1} + n_i x_{i-1}^{\Delta} + x_{i-1}^{\Delta-1}) \\ &= O(d_i[n_{i-1}^{2\,\delta-\Delta-1} + n_{i-1}^{\delta-\Delta} + n_{i-1}^{1-\Delta}]) = O(d_i n_{i-1}^{2\,\delta-\Delta-1}) . \end{aligned} \tag{3.24}$$

Let us suppose that $x_i \leqq t < x_{i-1}$. Then

$$\begin{aligned} \int_0^t \mid du^{\Delta}\varphi(u) \mid &= \sum_{j=i}^{\infty} \mid J(x_j) \mid + \sum_{j=i+1}^{\infty} \int_{x_j}^{x_{j-1}} \mid \xi'(u) \mid du \\ &+ \int_{x_i}^{t} \mid \xi'(u) \mid du = I_1 + I_2 + I_3 . \end{aligned} \tag{3.25}$$

But, if $\delta \leqq \Delta$, from (3.23)

$$I_1(t) = O\left(\sum_{j=1}^{\infty} d_j\, n_j^{-1}\right) = o(n_i^{-1}) = o(t)$$

and if $\delta \leqq \dfrac{\Delta + 1}{2}$, from (3.24)

$$I_2(t) = O\left(\sum_{j=i+1}^{\infty} d_j\, n_{j-1}^{-1}\right) = o(n_i^{-1}) = o(t) .$$

Finally, if $\delta \leqq \dfrac{\Delta + 1}{2}$

$$I_3(t) = o\left(\int_{x_i}^{t} n_{i-1}^{2\,\delta-\Delta-1}\right) = o(t) .$$

Therefore, if $\delta \leqq \dfrac{\Delta + 1}{2}$, $\varphi_{\Delta}(t) = o(t)$ as $t \to 0$.

13. Now we shall prove that the Fourier series of $f(x)$ does not converge at $x = 0$. We use the formula

$$S_{n_i}(t) = \frac{1}{\pi}\int_0^\pi f(t)\,\frac{\sin\,(n_i + 1/2)t}{\sin t/2}\,dt$$

$$= -\frac{1}{\pi}\int_0^{x_i} F(t)\left\{\frac{(n_i + 1/2)\sqrt{\cos\,(n_i + 1/2)t}}{\sin t/2} - \frac{\cos t/2 \sin\,(n_i + 1/2)t}{2\sin^2 t/2}\right\}dt$$

$$(3.26) \qquad -\frac{1}{\pi}\int_{x_i}^{x_{i-1}} F(t)\,\frac{(n_i + 1/2)\cos\,(n_i + 1/2)t}{\sin t/2}\,dt + \frac{1}{2\pi}\int_{x_i}^{x_{i-1}} F(t)\,\frac{\cos t/2 \sin\,(n_i + 1/2)t}{\sin^2 t/2}\,dt$$

$$+ \frac{1}{\pi}\int_{x_{i-1}}^{\pi} f(t)\,\frac{\sin\,(n_i + 1/2)t}{\sin t/2}\,dt = I_1 + I_2 + I_3 + I_4\,.$$

By (3.09)

$$(3.27) \qquad |\,I_4\,| < 1\,,$$

if $d_i \neq 0$. Also

$$(3.29) \qquad I_1 = o\left(n_i\int_0^{x_i} dt\right) = o(1) \text{ as } i \to \infty\,.$$

Since $d_i = o((\log 1/x_i)^{-1})$,

$$(3.29) \qquad I_3 = O\left(d_i\int_{x_i}^{x_{i-1}} \frac{dt}{t}\right) = O\left(di\,\frac{x_i}{x_{i-1}}\right) = o(1) \text{ as } i \to \infty\,.$$

Finally

$$I_2 = -\frac{1}{\pi}\int_{x_i}^{x_{i-1}} F(t)\,\frac{(n_i + 1/2)\,(\cos n_i t \cos t/2 - \sin n_i t \sin t/2)}{\sin t/2}\,dt$$

$$= -\frac{2}{\pi}\int_{x_i}^{x_{i-1}} F(t)\,\frac{\cos n_i t}{t}\,dt + o(1)\,,$$

and for i sufficiently large, by (3.09) and (3.01)

$$d_i > \left(\frac{1}{n_i}\right)^{\frac{1-\delta}{2\delta}}\,, \qquad \textit{if } d_i \neq 0\,,$$

so that, for such i,

$$I_2 = -\frac{2}{\pi}\,d_i\int_{x_i}^{x_{i-1}} n_i \cos^2 n_i t\,dt + o(1)$$

$$(3.30) \qquad = -\frac{d_i\,n_i}{\pi}\int_{x_i}^{x_{i-1}} (1 + \cos 2\,n_i t)\,dt + o(1)$$

$$= -\frac{1}{\pi}\,d_i\,n_i\,x_{i-1} + o(1) = -\frac{1}{\pi}\,d_i\,\epsilon_i^{-1/\delta}\,n_i^{1-1/\delta} + o(1) \to -\infty \text{ as } i \to \infty\,.$$

Therefore

$$S_{n_i}(0) \to -\infty \text{ as } i \to \infty\,, \qquad \textit{if } d_i \neq 0$$

and the Fourier series of $f(x)$ does not converge at $x = 0$.

BROWN UNIVERSITY.

REFERENCES

[1] S. BOCHNER, *Vorlesungen über Fouriersche Integrale*, Leipzig 1932.

[2] H. HAHN, *Über Fejér's Summierung der Fourierschen Reihen*, Jahresberichte der Deutschen Math. Vereinigung, Vol. 25 (1916), pp. 359–366.

[3] G. H. HARDY, *Notes on some points in the integral calculus*, LV, Messenger of Math., Vol. 51 (1922), pp. 186–192.

[4] G. H. HARDY AND J. E. LITTLEWOOD, *Some new convergence criteria for Fourier series*, Annali della R. Scuola Normale Superiore de Pisa, (2) Vol. 3 (1934), pp. 43–62.

[5] E. HILLE AND J. D. TAMARKIN, *On the summability of Fourier series*, I, Trans. Amer. Math. Soc., Vol. 34 (1932), pp. 757–783.

[6] E. HILLE AND J. D. TAMARKIN, *On the summability of Fourier series*, V, Proc. Nat. Ac.

[7] R. E. A. C. PALEY, W. C. RANDELS AND M. F. ROSSKOPF, *On the summation of Fourier series*, Bull. Amer. Math. Soc., Vol. 40 (1934), pp. 69–74.

Annals of Mathematics
Vol. 36, No. 4, October, 1935

DIVISION BY NON-SINGULAR MATRIC POLYNOMIALS

By Merrill M. Flood

(Received May 1, 1934; Revised January 2, 1935)

1. **Introduction.** A matrix P, whose elements are polynomials in a scalar variable λ with coefficients in a commutative field, may be written in the form $P = \sum_{i=0}^{p} P_i\lambda^i$, $P_p \neq 0$, and is called a "matric polynomial" of "degree" p (or simply "polynomial" when there is no ambiguity). It is sufficient to consider the "constant" matrices P_i square and of the same order θ.

If $D = \sum_{i=0}^{d} D_i\lambda^i$, $| D_d | \neq 0$, is a second such polynomial, it is well known[1] that there exist unique matric polynomials Q, R, Q^1, and R^1, of which Q and Q^1 are each identically zero or of degree $p - d$ and R and R^1 are each of degree less than d, such that $P = QD + R = DQ^1 + R^1$. K. Hensel[2] has extended this result to the case in which $| D_d | = 0$ but $| D | \neq 0$. J. H. M. Wedderburn notes that in this case the quotient and remainder are not necessarily unique and the degree of the quotient may be greater than $p - d$. These results follow readily from those given in this paper.

In his lectures on matrices at Princeton University Professor Wedderburn proposed this exercise: Given any non-singular matric polynomial D, to find the degree of the matric polynomial H of minimum degree, such that HD has the same degree as D and also has a non-singular leading coefficient. Its solution is included here but is incidental to this study of the division transformation to which it led. I take this opportunity to thank Professor Wedderburn for the interest he has shown in this paper by reading the manuscript and for helpful suggestions made as it was being written.

In the first part of this paper it is my purpose to show how all divisions of a matric polynomial P by a non-singular matric polynomial D may be found. A linear basis will be found for the quotients and some properties of the quotients and remainders thus found will also be given. It is sufficient to consider dextro-lateral division. In the second part of the paper a canonical form is given for a matric polynomial subjected to elementary transformations by constant matrices and a close study is made of the linear case with its connection to the division transformation.

2. **Notation and definitions.** An upper case Roman letter with or without superscripts will only be used to denote a matric polynomial and the corresponding lower case letter with the same superscripts will denote the degree of the polynomial. We will write $D^- = \sum_{\alpha=0}^{d^-} D_\alpha^-\lambda^\alpha$ and $D^* = \sum_{\beta=0}^{d^*} D_\beta^*\lambda^\beta$ where D^-

---

[1] Wedderburn, J. H. M.: *Lectures on Matrices*, p. 21, 22. American Mathematical Society Colloquium Publications, Vol. 17, 1934.

[2] Kronecker, L.: *Vorlesungen über Determinantentheorie*, Vol. I, p. 364, Leipzig 1903.

and D^* denote the adjoint and determinant of D respectively. The rank of D will be denoted by $\rho\{D\}$ and the degree of D will be denoted by $\delta\{D\}$ as well as by d.

We will denote by $\mathbf{Q}^{pd}$ and $\mathbf{R}^{pd}$ the classes of all polynomials $Q^{pd\alpha}$ and $R^{pd\alpha}$, respectively, which satisfy the relations $P = Q^{pd\alpha}D + R^{pd\alpha}$, $\delta\{R^{pd\alpha}\} < \delta\{D\}$. (The range of α is not necessarily denumerable). Any such relation is called a "dextro-lateral division of P by D" or simply "division of P by D."

The polynomial D is "proper" if D_d is non-singular.[3] D is "strictly proper" if $D_d = 1$, the identity matrix.

We say that "D is left [right] proper with C" if DC [CD] is proper. "D is strictly left [right] proper with C" if DC [CD] is strictly proper.

We say that "D left [right] reduces C" if $\delta\{DC\} < c$ [$\delta\{CD\} < c$]. The meanings of "properly left [right] reduces" and "strictly properly left [right] reduces" are evident. The class of polynomials $R^{d\sigma}$ which left reduce D will be denoted by $\mathbf{R}^d$.

We say that "D is left [right] associated with C" if $\delta\{DC\} = c$ [$\delta\{CD\} = c$] and DC [CD] is proper. Also, "D is strictly left [right] associated with C" if $\delta\{DC\} = c$ [$\delta\{CD\} = c$] and DC [CD] is strictly proper. The class of polynomials $A^{d\sigma}$ which are strictly left associated with D will be denoted by $\mathbf{A}^d$.

The quantity $d + d^- - d^*$ will be called the "deficiency" of D and will be denoted by $\Delta\{D\}$.

3. Existence of division for non-singular polynomials.

(3.1) Theorem. *If P is any matric polynomial and D is any non-singular matric polynomial, there exists one and only one pair of matric polynomials Q^{pd0} and R^{pd0} such that $P = Q^{pd0}D + R^{pd0}$, $r^{pd0} < d$, and $\delta\{R^{pd0}D^-\} < d^*$.* (Of course we suppose $d^* > 0$ so that D is not a unit.)

Proof: There exists one and only one pair of polynomials Q and R such that $PD^- = QD^* + R$ where $r < d^*$. If both members of this equation are multiplied by D and divided by the non-zero scalar polynomial D^* we obtain $P = QD + (RD/D^*)$. Since (RD/D^*) is necessarily a matric polynomial and of lower degree than D the truth of the first part of the theorem is apparent when we set $Q^{pd0} = Q$ and $R^{pd0} = (RD/D^*)$ and the second part follows immediately.

(3.11) Corollary. $q^{pd0} = \delta\{PD^-\} - d^*$ *if and only if* $\delta\{PD^-\} \geqq d^*$.

(3.12) Corollary. $Q^{pd0} = 0$ *if and only if* $\delta\{PD^-\} < d^*$.

4. Determinations of all divisions of P by D.

(4.1) Theorem. *If $\mathbf{T}$ is the class of all strictly proper polynomials T^σ of degree d, and if $\mathbf{Q}$ is the class of all quotients $Q^{t^\sigma d0}$ obtained by dividing each member of $\mathbf{T}$ by D, then $\mathbf{Q} = \mathbf{A}^d$.*

Proof: Obviously $\mathbf{Q} \subset \mathbf{A}^d$. Now we may write $A^{d\alpha}D = T^\alpha \subset \mathbf{T}$. This

[3] MacDuffee, C. C.: *The Theory of Matrices*, p. 45. Ergebnisse der Mathematik, vol. 5, 1933.

gives $T^{\alpha}D^{-} = A^{d\alpha}D^{*}$ and it follows by (3.1) then that $\mathbf{A}^d \subset \mathbf{Q}$. The theorem now follows since both $\mathbf{Q} \subset \mathbf{A}^d$ and $\mathbf{A}^d \subset \mathbf{Q}$.

(4.11) Corollary. $\quad a^{d\alpha} = \Delta\{D\}$.

(4.12) Corollary. $\quad A^{d\alpha}_{\Delta\{D\}} = D^{-}_{d^{-}}/D^{*}_{d*}$.

We may now find all divisions of a polynomial P by a non-singular polynomial D. Set $T^0 = \lambda^d$ and $T^{\sigma} = Q^{t^{\sigma}d0}D + R^{t^{\sigma}d0}$.

(4.2) Theorem. *If P and D are matric polynomials, D non-singular, then all divisions of P by D are given by*

$$P = (Q^{pd0} + Q^{t^{\gamma}d0} - Q^{t^0d0})D + (R^{pd0} - [Q^{t^{\gamma}d0} - Q^{t^0d0}]D).$$

Proof: We may write $P = Q^{pd0}D + R^{pd0}$ by (3.1). Obviously, the equations of the theorem constitute divisions of P by D. Suppose now, that $P = MD + N$, $n < d$, is any division of P by D. Certainly then, $(M - Q^{pd0})D = (R^{pd0} - N)$ and since $\delta\{R^{pd0} - N\} < d$ the polynomial $(Q^{t^0d0} + M - Q^{pd0})$ must belong to $\mathbf{A}^d$. We may now set $Q^{t^{\beta}d0} = Q^{t^0d0} + M - Q^{pd0}$ and therefore $M = Q^{pd0} + Q^{t^{\beta}d0} - Q^{t^0d0} = Q^{pd^{\gamma}}$ and $N = R^{pd0} + (Q^{t^0d0} - Q^{t^{\beta}d0})D = R^{pd^{\gamma}}$ and the theorem follows.

In particular, to find all polynomials which left reduce D we only need to set $P = 0$ in (4.2) and find the class $\mathbf{Q}^{pd}$. A simple method for actually constructing the set $\mathbf{R}^d$ is contained in the following theorem:

(4.3) Theorem. *If, for $(i = 0, 1, \cdots, d)$, $P^i = \lambda^i$, then the polynomial $R \subset \mathbf{R}^d$ if and only if there exist constant matrices M_i such that $R = \sum_{i=0}^{d-1} M_i Q^{p^i d0}$ and we may say that the polynomials $Q^{p^i d0}$ form a "linear basis" for the set $\mathbf{R}^d$.*

Proof:[4] It is clear that any linear combination of the polynomials $Q^{p^i d0}$ belongs to $\mathbf{R}^d$. Now if $R \subset \mathbf{R}^d$ we may write
$RD = M = \sum_{i=0}^{d-1} M_i\,[Q^{p^i d0}D + R^{p^i d0}]$. Since $\delta\,\{\sum_{i=0}^{d-1} M_i\, R^{p^i d0}D^{-}\} < d^*$ it follows by (3.1) that $\sum_{i=0}^{d-1} M_i\, Q^{p^i d0} = Q^{md0} = R$ and our proof is completed

(4.31) Corollary. $\quad Q^{p^{\alpha}d0} = 0$ *if and only if* $d > \Delta\{D\}$ *and for* $(\alpha = 0, 1, \cdots d - 1 - \Delta\{D\})$.

(4.32) Corollary. $\quad q^{p^{\alpha}d0} = \alpha - d + \Delta\{D\}$ *if and only if* $\alpha \geqq d - \Delta\{D\}$.

(4.4) Lemma. (i)
$$\sum_{\beta=0}^{d} D_{\beta}\, Q^{p^{\beta}d0} = 1$$

and

(ii)
$$\sum_{\beta=0}^{d} D_{\beta}\, R^{p^{\beta}d0} = 0\,.$$

Proof: $D = \sum_{\beta=0}^{d} D_{\beta}\, \lambda^{\beta} = \sum_{\beta=0}^{d} D_{\beta}\, (Q^{p^{\beta}d0}D + R^{p^{\beta}d0}) = (\sum_{\beta=0}^{d} D_{\beta}\, Q^{p^{\beta}d0})\, D + (\sum_{\beta=0}^{d} D_{\beta}\, R^{p^{\beta}d0})$. Since $\delta\{\sum_{\beta=0}^{d} D_{\beta}\, R^{p^{\beta}d0}D^{-}\} < d^*$ it follows immediately by (3.1) that $\sum_{\beta=0}^{d} D_{\beta}\, R^{p^{\beta}d0} = R^{dd0} = 0$ and $\sum_{\beta=0}^{d} D_{\beta}\, Q^{p^{\beta}d0} = Q^{dd0} = 1$.

As a matter of fact, if we set $E = P^{x}D$, then $\Delta\{E\} = \Delta\{D\}$ and $\mathbf{R}^d = \mathbf{R}^e$ for

[4] This proof is due to J. B. Rosser.

all positive integral values of x, so we may suppose x so large that $e \geqq \Delta\{E\}$ and $e^* \geqq e^- \geqq \Delta\{E\}$ and it is sufficient to consider the case in which this is true. Now set $B^{ek} = Q^{p\,e-\Delta\{E\}+k\,e0}$ and $V^{ek} = (\sum_{\beta=0}^{k} E^-_{e^- -k+\beta}\,\lambda^\beta)$ for $(k = 0, 1, \cdots, \Delta\{E\})$. It follows immediately from this definition of B^{ek} for $(k = 0, 1, \cdots, \Delta\{E\} - 1)$ and by (4.3) and (4.32) that the polynomials B^{ek} form a linear basis for the class $\mathbf{R}^e = \mathbf{R}^d$ and are of degree k.

(4.5) LEMMA. $B^{ek}_{k-j} = B^{em}_{m-j}$ *for* $(0 \leqq k \leqq m \leqq \Delta\{E\}; 0 \leqq j \leqq k)$.

PROOF: We easily see from the definition of B^{ek} that $\lambda^{k+e-\Delta\{E\}}E^- = B^{ek}E^* + R^{p\,k+e-\Delta\{E\}\,e0}\,E^-$ for $(k = 0, 1, \cdots, \Delta\{E\})$ and from this $\sum_{h=0}^{k} [E^-_{e^- -h} - \sum_{j=0}^{h} B^{ek}_{k-j}\,E^*_{e^*+j-h}]\,\lambda^h = 0$. Hence

(4.51) $E^-_{e^- -h} - \sum_{j=0}^{h} B^{ek}_{k-j}\,E^*_{e^*+j-h} = 0$ for $(k = 0, 1, \cdots, \Delta\{E\}; h = 0, 1, \cdots, k)$ from which it follows that

$$\sum_{j=0}^{h} [B^{ek}_{k-j} - B^{em}_{m-j}]\,E^*_{e^*+j-h} = 0 \text{ for } (0 \leqq k \leqq m \leqq \Delta\{E\}; 0 \leqq h \leqq k)$$

and since $E^*_{e^*} \neq 0$ our lemma follows.

(4.6) THEOREM. *The polynomials* V^{ek} *for* $(k = 0, 1, \cdots, \Delta\{E\} - 1)$ *form a linear basis for* $\mathbf{R}^e$.

PROOF: It is easily seen that $V^{ek} \subset \mathbf{R}^e$ for $(k = 0, 1, \cdots, \Delta\{E\} - 1)$. It only remains to show that there exist constant matrices M^i_j such that $B^{ei} = \sum_{j=0}^{\Delta\{E\}-1} M^i_j V^{ej}$ for $(i = 0, 1, \cdots, \Delta\{E\} - 1)$. Now if we multiply (4.51) through by λ^{k-h} and sum on h from 0 to k we get, by means of (4.5), $V^{ek} = \sum_{p=0}^{k} \sum_{\beta=0}^{p} B^{e\,k-p+\beta}_{k-p} E^*_{\beta+e^*-p}\lambda^{k-p}$ and this may be written in the form

$$(4.61) \qquad V^{ek} = \sum_{\alpha=0}^{k} B^{ek-\alpha}E^*_{e^*-\alpha} \qquad \text{for} \qquad (k = 0, 1, \cdots, \Delta\{E\}).$$

Since $E^*_{e^*} \neq 0$ the matrix of this set of equations is non-singular. Hence they can be solved to yield the result desired and our proof is complete.

(4.7) THEOREM. *If D is non-singular, division of P by D is unique if and only if D is proper.*

PROOF: We need only show that the division is not unique if D is not proper. This follows immediately since $P = Q^{pd0}D + R^{pd0}$ and $P = (Q^{pd0} + D^-_{d^-})D + (R^{pd0} - D^-_{d^-}D)$ are distinct divisions of P by D.

5. On the degree of the quotient.

(5.1) THEOREM. *If D is non-singular, $q^{pd\gamma} = q^{pd0}$ for all values of γ if and only if either: (i) $q^{pd0} \geqq \Delta\{D\}$, or (ii) $q^{pd0} = \Delta\{D\} - 1$ and $\rho\{D^-_{d^-}\} < \rho\{\| D^-_{d^-} \mid P^1_{p^1} \|\}$, where $P^1 = PD^-$ and $\| M \mid N \|$ denotes the 2θ by θ matrix whose rows are the rows of M and N.*

PROOF: The theorem is obviously true if $\Delta\{D\} = 0$. If $q^{pd0} < \Delta\{D\} - 1$ then the polynomial $Q^{pd0} + V^{e\Delta\{D\}+1} \subset \mathbf{Q}^{pd}$ and is of degree $\Delta\{D\} - 1$. Also if $q^{pd0} > \Delta\{D\} - 1$ it follows immediately from (4.12) and (4.2) that $q^{pd\alpha} = q^{pd0}$. Finally, if $q^{pd0} = \Delta\{D\} - 1$ we must have $q^{pd\alpha} = q^{pd0}$ for all values of α unless there exists a polynomial $Q^{t\beta d0}$ such that

$$Q^{pd0}_{q\,pd0} + Q^{t^\beta d0}_{q\,t^\beta d0_{-1}} - Q^{t^0 d0}_{q\,t^0 d0_{-1}} = 0 .$$

We find that this is possible if and only if there exists a constant matrix T^γ_{d-1} such that $T^\gamma_{d-1}D^-_{d^-} + P^1_{p^1} = 0$. This is possible if and only if[5]

$$\rho\{D^-_{d^-}\} = \rho\{\|\, D^-_{d^-} \mid P^1_{p^1} \,\|\} .$$

(5.11) COROLLARY. *If D is not proper but $\delta\{PD^-\} = p + d^-$ then $q^{pd\gamma} = q^{pd0}$ if and only if $q^{pd0} \geqq \Delta\{D\}$.*

(5.2) THEOREM. *If P is proper and D is non-singular but not proper, then $q^{pd\gamma} = q^{pd0}$ for all values of γ if and only if $p \geqq d$.*

PROOF: (i) If $p \geqq d$ then $\delta\{PD^-\} - d^* = p - d + \Delta\{D\} \geqq 0$ so by (3.11) $q^{pd0} = p - d + \Delta\{D\} \geqq \Delta\{D\}$ and so by (5.1) $q^{pd\gamma} = q^{pd0}$ for all values of γ.

(ii) If $q^{pd\gamma} = q^{pd0}$ for all values of γ, then by (5.11) $q^{pd0} \geqq \Delta\{D\}$. By (3.11) and (3.12) either $Q^{pd0} = 0$ or $q^{pd0} = p - d + \Delta\{D\}$ according as $p - d + \Delta\{D\}$ is negative or not. But $Q^{pd0} = 0$ is clearly impossible if $q^{pd\gamma} = q^{pd0}$ for all values of γ since D is improper. Hence we must have $q^{pd0} = p - d + \Delta\{D\} \geqq \Delta\{D\}$ from which we see that $p \geqq d$ and our proof is complete.

(5.21) COROLLARY. *If D is not proper but $\delta\{PD^-\} = p + d^-$ then $q^{pd\gamma} = q^{pd0}$ for all γ only if $p \geqq d$.*

PROOF: Precisely the same as that for the second part of (5.2).

(5.3) LEMMA. *If $D^* \neq 0$ and $B \neq 0$ then $\delta\{BD\} \geqq b + d - \Delta\{D\}$ and the equality will hold if and only if $\delta\{BD^*\} = \delta\{BD\} + d^-$. In particular, then, the equality will hold if BD is proper.*

PROOF: If we set $BD = M$ then $BD^* = MD^- \neq 0$ so that $b + d^* = \delta\{MD^-\} \leqq m + d^-$, and the equality holds if and only if $\delta\{MD^-\} = m + d^-$. The theorem follows.

(5.4) THEOREM. *If $p \geqq d$ then $p - d \leqq q^{pd\gamma} \leqq p - d + \Delta\{D\}$.*

PROOF: From $P = Q^{pd\gamma}D + R^{pd\gamma}$, $r^{pd\gamma} < d$, we have immediately $Q^{pd\gamma}D^* = (P - R^{pd\gamma})D^-$, $\delta\{P - R^{pd\gamma}\} = p$. Then, since neither $Q^{pd\gamma}$ nor D^* is zero, we must have

$$q^{pd\gamma} = \delta\{(P - R^{pd\gamma})D^-\} - d^*. \tag{5.41}$$

Hence, by (5.3), $q^{pd\gamma} \geqq p + d^- - \Delta\{D\} - d^* = p - d$ which shows the first part of the theorem. The second part follows similarly from (5.41) since $\delta\{(P - R^{pd\gamma})D^-\} \leqq p + d^-$.

(5.5) LEMMA. *If DB is proper, then $\Delta\{D\} = \Delta\{B\}$.*

PROOF: Set $DB = T$. Then $D^*B = D^-T$ and $DB^* = TB^-$ so that $d^* + b = d^- + t$ and $d + b^* = t + b^-$. The lemma follows.

(5.6) THEOREM. *If $p \geqq d + \Delta\{D\}$ then $q^{pd0} = q^{pd\gamma}$.*

PROOF: By (5.3) and (5.5) our first hypothesis yields the relation $\delta\,\{PD^-\} - d^* \geqq p + d^- - \Delta\{D^-\} - d^* = p - d \geqq \Delta\{D\}$. So by (3.11) it follows that $q^{pd0} \geqq \Delta\{D\}$ and now by (5.1) that $q^{pd0} = q^{pd\gamma}$.

---

[5] Frobenius: J. reine angew. Math., vol. 84 (1878), p. 8.

6. On the remainders.

(6.1) THEOREM. $r^{pd\gamma} \geqq d - \Delta\{D\}$ *if* $\gamma \neq 0$.

PROOF: Since $\gamma \neq 0$ we must have as a consequence of (3.1) that $\delta\{R^{pd\gamma}D^-\} \geqq d^*$. But clearly $\delta\{R^{pd\gamma}D^-\} \leqq r^{pd\gamma} + d^-$ and so combining these inequalities $r^{pd\gamma} \geqq d^* - d^- = d - \Delta\{D\}$.

(6.11) COROLLARY. *If* $r^{pd\gamma} < d - \Delta\{D\}$ *then* $\gamma = 0$.

(6.2) THEOREM. *If* $\delta\{R^{pd0}D^-\} = r^{pd0} + d^-$ *or if* $R^{pd0} = 0$, *then* $r^{pd0} < r^{pd\gamma}$ *if* $\gamma \neq 0$.

PROOF: By (3.1) it follows that $r^{pd0} + d^- < d^*$ and therefore $r^{pd0} < d - \Delta\{D\}$. Hence, by (6.1), $r^{pd0} < r^{pd\gamma}$ if $\gamma \neq 0$. The theorem is obviously true if $R^{pd0} = 0$.

(6.21) COROLLARY. *If* $\delta\{R^{pd0}D^-\} = r^{pd0} + d^-$ *then* $r^{pd0} < d - \Delta\{D\}$ *and also* $\Delta\{D\} < \delta\{D\}$.

PROOF: The first statement was proved in the course of the proof given for the theorem and the second statement is obvious since R^{pd0} is a matric polynomial and therefore $r^{pd0} \geqq 0$.

(6.3) THEOREM. *If* $\delta\{R^{pd0}D^-\} = r^{pd0} + d^-$ *and if* L *properly left reduces* D, *then* $r^{pd0} < \delta\{LD\}$ *and there exists a remainder* $R^{pd\gamma}$ *which is proper.*

PROOF: Set $LD = S$ and then of course $(S_s)^* \neq 0$ and $s < d$. Now by (5.3) $s = l + d - \Delta\{D\}$ so that $s \geqq d - \Delta\{D\}$. Now consider the relation $P = Q^{ps0}S + R^{ps0}$, $r^{ps0} < s$. From this we obtain the division of P by D: $P = [(Q^{ps0} - 1)L]D + [R^{ps0} + S] = Q^{pd\gamma}D + R^{pd\gamma}$. Clearly $r^{pd\gamma} = s \geqq d - \Delta\{D\}$ and since $R^{pd\gamma}$ is proper it follows by (6.21) that $R^{pd\gamma} \neq R^{pd0}$ and $r^{pd0} < d - \Delta\{D\}$ so finally $r^{pd0} < r^{pd\gamma} = s$.

(6.4) THEOREM. $r^{pd0*} < d^*$.

PROOF: The theorem is trivial if $R^{pd0*} = 0$. If $R^{pd0*} \neq 0$ then $\delta\{(R^{pd0}D^-)^*\} = r^{pd0*} + d^{-*} = r^{pd0*} + (\theta - 1)d^*$. As a consequence of Theorem 3.1 we likewise get $\delta\{R^{pd0}D^-)^*\} \leq \theta\delta\{R^{pd0}D^-\} < \theta d^*$ and so our theorem follows.

(6.41) COROLLARY. If R^{pd0} is proper then $r^{pd0} < d^*/\theta$.

7. The associate forms of a matric polynomial.

In this part of the paper we investigate the form which a matric polynomial takes when it is multiplied on right and left by non-singular constant matrices. We find that it is possible, by a suitable choice of these two matrices, to put the polynomial into a form where it satisfies a set of rather restrictive conditions. The method of proof is constructive so we may assume that the polynomial satisfies this set of conditions in any case where the nature of the problem is such that multiplication by constant non-singular matrices yields an equivalent problem.

Let θ and φ be any positive integers. Let g_k for $(k = 1, 2, \cdots, \theta)$ be non-negative integers such that $\sum_{k=1}^{\theta} g_k = \varphi$. Let e_j for $(j = 1, 2, \cdots, \varphi)$ be square matrices of order φ with unity in the j^{th} row and column but zeros elsewhere. Finally, set

$$(7.1)\quad E_k = \left(\sum_{\alpha=0}^{g_k} e_{g_1+g_2+\cdots+g_{k-1}+\alpha}\right) - e_{g_1+g_2+\cdots+g_{k-1}} \quad \text{for } (k = 1, 2, \cdots, \theta)$$

and as an immediate consequence of this definition we see that $\sum_{k=1}^{\theta} E_k = 1$ and $E_kE_h = \delta_{kh}E_h$ where δ_{kh} is the well-known Kronecker symbol. These properties will be used frequently and without further comment.

If B is any square matrix of order φ we may set

$$B_{hm} = E_hBE_m \text{ for } (h, m = 1, 2, \cdots, \theta). \tag{7.2}$$

In particular, if $B = \sum_{\alpha=-\infty}^{+\infty} B_\alpha\lambda^\alpha$ denotes a matric polynomial of degree b and order φ so that $B_\alpha = 0$ if $\alpha > b$ or $\alpha < 0$ and $B_b \neq 0$, we may define matrices B_{jkhm}, for $(h, m = 1, 2, \cdots, \theta)$ and k any non-negative integer, by the relations:

$$\begin{gathered} B_{-1\,khm} = B_{okhm} = E_hB_{b-k}E_m \\ B_{jkhm} = B_{j-1\,khm} - \sum_{\alpha=1}^{j} [B_{\alpha-1\,k-j-1+\alpha\,h\alpha}\, B_{j-1\,j\alpha m}] \\ \text{for } (j = 1, 2, \cdots, \theta;\, j < k). \end{gathered} \tag{7.3}$$

(7.4) THEOREM. *If B is a matric polynomial and g a non-negative integer, there exist constant non-singular matrices P and Q and non-negative integers g_k for $(k = 1, 2, \cdots, g + 2)$ such that the polynomial $A = PBQ$ satisfies the relations:*

$$A_{k-2\,k-1\,mn} = E_mE_kE_n \text{ for } (k = 1, 2, \cdots, g + 1; m, n = k, k + 1, \cdots, g + 2).$$

PROOF: In case $g = 0$, we choose $g_1 = \rho\{B_b\}$, $g_2 = \varphi - g_1$, and P and Q so that $PB_bQ = E_1$. Our theorem is satisfied by this choice of P and Q and this choice only for g_k.

We suppose the theorem true for $g = t \geqq 0$. Then there exist constant non-singular matrices P^t and Q^t, and integers g_k^t for $(k = 1, 2, \cdots, t + 2)$ such that $A^t = P^tBQ^t$ satisfies the relation:

$$A^t_{k-2\;k-1\;m\;n} = E^t_mE^t_kE^t_n \text{ for } (k = 1, 2, \cdots, t + 1; m, n = k, k + 1, \cdots, t + 2). \tag{1}$$

We set $g_k = g_k^t$ for $(k = 1, 2, \cdots, t + 1)$, $g_{t+2} = \rho\{A^t_{t\;t+1\,t+2\,t+2}\}$, and $g_{t+3} = \varphi - \sum_{k=1}^{t+2} g_k$. We may choose constant non-singular matrices R and S such that $E^t_mRE^t_n = E^t_mSE^t_n = E^t_mE^t_n$ for $(m, n = 1, 2, \cdots, t + 2; m, n, t + 2 \neq)$ and $E^t_{t+2}RA^t_{t\;\;t+1\;\;t+2\;\;t+2}SE^t_{t+2} = E_{t+2}$ and we set $P = RP^t$ and $Q = Q^tS$ and $A = PBQ$.

It follows from these definitions that

$$A_{0\;k-1\;m\;n} = A^t_{0\;k-1\;m\;n} \text{ for } (m, n = 1, 2, \cdots, t + 1).$$

Now, the recursive relation (7.3) is of such a nature that any matrix B_{jkmn} can be expressed entirely in terms of matrices $B_{0\alpha\beta\gamma}$ and this relation takes the form of a sum, each of whose terms is a product of matrices $B_{0\alpha\beta\gamma}$. We write this relation as

$$B_{jkmn} = \sum_p{}' \prod_{\alpha=0}^{p} B_{0\,\mu^p_\alpha\,\sigma^p_\alpha\,\sigma^p_{\alpha+1}}, \qquad p = p(j, k, m, n) \tag{2}$$

where, as a consequence of the form of (7.3), we necessarily have

$$\sigma_0^p = m,\ \sigma_{p+1}^p = n,\ \sigma_\alpha^p \leqq j \text{ for } (\alpha = 1, 2, \cdots, p),$$
$$\text{and } \mu_\alpha^p \leqq k \text{ for } (\alpha = 0, 1, \cdots, p).$$

A simple application of these results yields

$$(3)\quad A_{k-2\ k-1\ m\ n} = A^t_{k-2\ k-1\ m\ n} \text{ for } (k = 1, 2, \cdots, t+3;\ m, n = 1, 2, \cdots, t+1).$$

Again, for $(m, n = t+2, t+3;\ k = 1, 2, \cdots, t+3)$, we may write

$$A_{k-2\,k-1\,m\,n} = \sum_p{}' \prod_{\alpha=0}^{p} A_{0\,\mu_\alpha^p\,\sigma_\alpha^p\,\sigma_{\alpha+1}^p}, \qquad p = p(k-2, k-1, m, n).$$

From this we obtain

$$A_{k-2\,k-1\,m\,n} = \sum_p{}' \Big\{ E_m E^t_{t+2} R E^t_{t+2} A^t_{b-\mu_0^p} E_{\sigma_1^p} \prod_{\alpha=1}^{p-1} A^t_{0\,\mu_\alpha^p\,\sigma_\alpha^p\,\sigma_{\alpha+1}^p} E_{\sigma_p^p} R A^t_{b-\mu_p^p} E^t_{t+2} S E^t_{t+2} E_n \Big\}$$

$$= E_m E^t_{t+2} R \left[\sum_{p'}{}' \prod_{\alpha=0}^{p} A^t_{0\,\mu_\alpha^{p'}\,\sigma_\alpha^{p'}\,\sigma_{\alpha+1}^{p'}} \right] S E^t_{t+2} E_n$$
$$\text{for } p' = p'(k-2, k-1, t+2, t+2).$$

Hence $A_{t\,t+1\,m\,n} = E_m E_{t+2} E_n$ for $(m, n = t+2, t+3)$. This relation combined with (1) and (3) gives

$$A_{k-2\ k-1\ m\ n} = E_m E_k E_n \text{ for } (k = 1, 2, \cdots, t+2;\ m, n = k, k+1, \cdots, t+3)$$

which is simply (1), the hypothesis of induction, with t replaced by $t+1$, and the theorem follows.

(7.41) COROLLARY. *$g_k = \rho\{A_{k-2\ k-1\ k\ k}\}$ for $(k = 1, 2, \cdots, g+1)$.*

Any polynomial A which satisfies the conditions of this theorem we call an "associate form" of B of "grade g."

8. The associate forms of a linear polynomial.

(8.1) THEOREM. *If B is any non-singular linear polynomial and A any associate form of B, of grade $g \geqq \Delta\{B\}$, then $\sum_{k=1}^{\Delta\{B\}+1} g_k = \varphi$, $g_{\Delta\{B\}+1} \neq 0$, and $g_k = 0$ for $(k = \Delta\{B\}+2, \Delta\{B\}+3, \cdots, g+2)$.*

PROOF: By definition, $A_{0h\,m\,n} = 0$ if $h > 1$. It follows immediately that $A_{j\ j+h\ m\ n} = 0$ if $h > 1$, for, suppose that $A_{j\ j+h\ m\ n} = 0$ for $(j = 0, 1, \cdots, p < g+2)$ if $h > 1$. Then by (7.3) and this hypothesis follows

$$A_{p+1\ p+1+h\ m\ n} = A_{p\ p+1+h\ m\ n} - \sum_{\alpha=1}^{p+1} A_{\alpha-1\ h+\alpha-1\ m\ \alpha} A_{p\ p+1\ \alpha\ n} = 0$$

and so we have shown

(1) $A_{j\,j+h\,m\,n} = 0$ for $(j = 0, 1, \cdots, g + 2; m, n = 1, 2, \cdots, g + 2)$ if $h > 1$.

It will be convenient to set

(2) $$(k - 1\ m\ n) = A_{k-1\,k\,m\,n} \text{ for } (k = 0, 1, \cdots, \infty).$$

With these definitions, we obtain from (7.3) as a consequence of (1)

(3) $(kmn) = -\sum_{\alpha=1}^{k}(\alpha - 1\ m\ \alpha)(k - 1\ \alpha\ n)$ for $(k, m, n = 1, 2, \cdots, g + 2)$.

We note now that $\sum_{\alpha=1}^{k} (\alpha - 1\ m\ \alpha)(k - 1\ \alpha\ n) = \sum_{\alpha=1}^{k} (k - 1\ m\ \alpha)(\alpha - 1\ \alpha\ n)$ if $k = 1$ and suppose it true for $(k = 1, 2, \cdots, p < g + 2)$. This hypothesis, with the aid of (3), gives

$$\sum_{\alpha=1}^{p+1} (\alpha - 1\ m\ \alpha)(p\ \alpha\ n) = (p\ m\ p+1)(p\ p+1\ n) - \sum_{\alpha,\beta=1}^{p} (\alpha - 1\ m\ \alpha)(\beta - 1\ \alpha\ \beta)(p - 1\ \beta\ n) = (p\ m\ p + 1)(p\ p + 1\ n) - \sum_{\alpha,\beta=1}^{p} (\alpha - 1\ m\ \alpha)(p - 1\ \alpha\ \beta)(\beta - 1\ \beta\ n) = \sum_{\alpha=1}^{p+1} (p\ m\ \alpha)(\alpha - 1\ \alpha\ n)$$

and so we have shown

(4) $(kmn) = -\sum_{\alpha=1}^{k} (k - 1\ m\ \alpha)(\alpha - 1\ \alpha\ n)$ for $(k, m, n = 1, 2, \cdots, g + 2)$.

Since A is an associate form of B of grade g we may write

(5) $(k - 2\ m\ n) = E_m E_k E_n$ for $(k = 1, 2, \cdots, g + 1; m, n = k, k + 1, \cdots, g + 2)$.

Clearly $\Delta\{A\} = \Delta\{B\}$, and since $B^* \neq 0$ there exists a polynomial $V = \sum_{\alpha=-\infty}^{+\infty} V_\alpha \lambda^\alpha$ of degree $v = \Delta\{A\}$ which is strictly left associated with A. Hence it must satisfy the relations

$$\sum_{\alpha=0}^{k} V_{v-\alpha} A_{a-k+\alpha} = \delta_{kv} \quad \text{for} \quad (k = 0, 1, \cdots, v)$$

and we may replace them by the equivalent set

$$\sum_{\alpha=0}^{k} \sum_{\beta=1}^{g+2} V_{v-\alpha} A_{0\,k-\alpha\,\beta\,m} = \delta_{kv} E_m \quad \text{for} \quad (k = 0, 1, \cdots, v; \quad m = 1, 2, \cdots, g + 2)$$

which in turn, as a consequence of (1), become simply

(6) $$\sum_{\alpha=1}^{g+2} [V_{v-k}(-1\ \alpha\ m) + V_{v-k+1}(0\ \alpha\ m)] = \delta_{kv} E_m \quad \text{for} \quad (k = 0, 1, \cdots, v; \quad m = 1, 2, \cdots, g + 2).$$

The theorem is obviously true if $\Delta\{B\} = 0$ so in what follows we assume that $\Delta\{B\} > 0$. Now the relation

$$(7) \quad \sum_{\beta=0}^{k} V_{v-\beta} \sum_{\alpha=k+1-\beta}^{g+2} (k - \beta - 1\, \alpha\, m) = \delta_{kv} E_m \quad \text{for} \quad (m = 1, 2, \cdots, g+2)$$

is easily verified for $k = 0$. We assume that it holds for $(k = 0, 1, \cdots, p < v)$. Since $v \leqq g$, we may set $m = k + 1$ in (7) and get as a consequence of (5)

$$(8) \qquad V_v E_k = 0 \qquad \text{for} \qquad (k = 1, 2, \cdots, p+1).$$

If we set $m = h - j + 1$ in (7) and use (5) we get

$$V_{v-j} E_{h-j+1} = - \sum_{\gamma=0}^{j-1} V_{v-\gamma} \sum_{\alpha=h+1-\gamma}^{g+2} (h - 1 - \gamma\, \alpha\, h - j + 1)$$
$$\text{for} \quad (j = 1, 2, \cdots, p;\ h = j, j+1, \cdots, p)$$

and if $k = h - j + 1$ and $\gamma = p + 1 - \beta$, this becomes

$$(9) \quad \begin{aligned} V_{v-j} E_k = - \sum_{\beta=p+2-j}^{p+1} \sum_{\alpha=k+j+\beta-p-1}^{g+2} V_{v+\beta-p-1} (k + j + \beta - p - 3\, \alpha\, k) \\ \text{for} \quad (j = 1, 2, \cdots, p+1;\ k = 1, 2, \cdots, p+1-j). \end{aligned}$$

For convenience, let us set

$$(10) \quad \begin{aligned} \Omega_h = \sum_{\beta=h}^{p+1} \sum_{\alpha=p+2-\beta}^{g+2} V_{v-\beta} (p - \beta\, \alpha\, m) \qquad \text{for} \qquad (h = 0, 1, \cdots, p+1; \\ m = 1, 2, \cdots, g+2). \end{aligned}$$

We may now rewrite (6) in the form

$$\Omega_{p+1} + \sum_{\alpha=1}^{g+2} V_{v-p} (0\, \alpha\, m) - \delta_{p+1\, v} E_m = 0 \qquad \text{for} \qquad (m = 1, 2, \cdots, g+2)$$

and with the help of (9) this becomes

$$(11) \quad \begin{aligned} \Omega_{p+1-m} - \sum_{\beta=m+1}^{p+1} V_{v-p-1+\beta} \sum_{\Delta=1}^{m} \sum_{\alpha=\beta}^{g+2} (\beta - 2\, \alpha\, \Delta)(\Delta - 1\, \Delta\, n) - \delta_{p+1\, v} E_n = 0 \\ \text{for} \quad (n = 1, 2, \cdots, g+2;\ m = 1). \end{aligned}$$

We suppose now that (11) holds for $(m = 1, 2, \cdots, r < p)$ and from this, with the help of (4), we obtain

$$\Omega_{p-r} - \sum_{\beta=r+2}^{p+1} V_{v-p-1+\beta} \sum_{\Delta=1}^{r} \sum_{\alpha=\beta}^{g+2} (\beta - 2\, \alpha\, \Delta)(\Delta - 1\, \Delta\, n) - V_{v-p+r} \sum_{\alpha=r+2}^{g+2} (r\, \alpha\, n)$$
$$- V_{v-p+r} \sum_{\Delta=1}^{r} \sum_{\alpha=r+1}^{g+2} (r - 1\, \alpha\, \Delta)(\Delta - 1\, \Delta\, n) - \delta_{p+1\, v} E_n = \Omega_{p-r}$$
$$- \sum_{\beta=r+2}^{p+1} V_{v-p-1+\beta} \sum_{\Delta=1}^{r} \sum_{\alpha=\beta}^{g+2} (\beta - 2\, \alpha\, \Delta)(\Delta - 1\, \Delta\, n) + V_{v-p+r}(r\, r+1\, n) - \delta_{p+1 v} E_n =$$
$$\Omega_{p-r} - \sum_{\beta=r+2}^{p+1} V_{v-p-1+\beta} \sum_{\Delta=1}^{r+1} \sum_{\alpha=\beta}^{g+2} (\beta - 2\, \alpha\, \Delta)(\Delta - 1\, \Delta\, n) - \delta_{p+1\, v} E_n = 0$$
$$\text{for} \qquad (n = 1, 2, \cdots, g+2).$$

Since this last equation is simply (11) with $m = r + 1$ it follows by our induction that

$$(12)\quad \Omega_{p+1-m} - \sum_{\beta=m+1}^{p+1} V_{v-p-1+\beta} \sum_{\Delta=1}^{m} \sum_{\alpha=\beta}^{g+2} (\beta - 2\,\alpha\,\Delta)\,(\Delta - 1\,\Delta\,n) - \delta_{p+1\,v}E_n = 0$$

$$\text{for } (n = 1, 2, \cdots, g + 2; m = 1, 2, \cdots, p).$$

Now if we set $m = p$ in (12) we get

$$\Omega_1 - V_v \sum_{\Delta=1}^{p} \sum_{\alpha=p+1}^{g+2} (p - 1\,\alpha\,\Delta)\,(\Delta - 1\,\Delta\,n) - \delta_{p+1\,v}E_n = 0$$

and if we use (10) and $V_vE_{p+1} = 0$ from (8) we obtain

$$\Omega_0 - V_v\left[\sum_{\Delta=1}^{p} \sum_{\alpha=p+2}^{g+2} (p - 1\,\alpha\,\Delta)\,(\Delta - 1\,\Delta\,n) + \sum_{\alpha=p+2}^{g+2} (p\,\alpha\,n)\right] - \delta_{p+1\,v}E_n = 0$$

and with the help of (4) it follows immediately from this that

$$\Omega_0 = \delta_{p+1\,v}E_n \text{ for } (n = 1, 2, \cdots, g + 2)$$

and since this is simply (7) with $k = p + 1$ it follows by our induction that

$$(13)\quad \sum_{\beta=0}^{k} V_{v-\beta} \sum_{\alpha=k+1-\beta}^{g+2} (k - \beta - 1\,\alpha\,m) = \delta_{kv}E_m$$

$$\text{for } (k = 0, 1, \cdots, v; m = 1, 2, \cdots, g + 2).$$

Finally, if we set $k = v$ in (13) and use (5) we get $E_m = \sum_{\beta=0}^{v} V_{v-\beta}E_{v+1-\beta}E_m$ for $(m = v + 1, v + 2, \cdots, g + 2)$. From this it is clear that $E_m = 0$ for $(m = v + 2, v + 3, \cdots, g + 2)$ and we have already seen that $V_vE_m = 0$ for $(m = 1, 2, \cdots, v)$. Hence $V_v = \sum_{m=1}^{g+2} V_vE_m = V_vE_{v+1} \neq 0$ and so $E_{v+1} \neq 0$ which completes the proof of our theorem.

(8.11) COROLLARY. *If A is any associate form of the linear non-singular polynomial B of grade $g < \Delta\{B\}$, then $g_{g+2} \neq 0$.*

PROOF: We suppose there does exist an associate form of B of grade $g < \Delta\{B\}$ such that $g_{g+2} = 0$. Then we may construct a new associate form of B by setting $g'_k = g_k$ for $(k = 1, 2, \cdots, g + 2)$ and $g'_k = 0$ for $(k = g + 3, g + 4, \cdots, \Delta\{B\} + 2)$. The polynomial A is still an associate form of B with this choice of g'_k but this situation clearly contradicts (8.1).

(8.12) COROLLARY. *Theorem (8.1) holds equally well for any non-singular polynomial B provided $B_{b-k} = 0$ for $(k = 2, 3, \cdots, \Delta\{B\})$.*

PRINCETON UNIVERSITY,
PRINCETON, NEW JERSEY.

ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

ON THE FACTORIZATION OF POLYNOMIALS TO A PRIME MODULUS

BY MORGAN WARD

(Received December 4, 1934)

1. Let

$$A(x) = x^N - a_1 x^{N-1} - a_2 x^{N-2} - \cdots - a_N$$

be a polynomial in x with rational integral coefficients[1] and N distinct roots, $\alpha_1, \alpha_2, \cdots, \alpha_N$ and let p be a prime which does not divide its discriminant. Then we have a unique factorization modulo p:

$$A(x) \equiv A_1(x)A_2(x) \cdots A_r(x) \pmod{p} \tag{1.1}$$

where the polynomials $A_i(x)$ are all distinct, and all irreducible modulo p. I give here two formulas connecting the degrees of the polynomials $A_i(x)$ with the powers of p dividing certain of the numbers

$$\Delta_{(n)}(A) = \prod_{\nu=1}^{N} (\alpha_\nu^{p^n} - \alpha_\nu) = \text{Res}\,\{x^{p^n} - x, A(x)\}, \; n \text{ a positive integer.} \tag{1.2}$$

These numbers have been studied recently by D. H. Lehmer in another connection.[2]

2. Let $\mathfrak{A}$ denote the residue class of all polynomials of degree N which are congruent to $A(x)$ modulo p, and consider for each polynomial $A'(x)$ of $\mathfrak{A}$ the highest power of p which divides $\Delta_{(n)}(A') = \text{Res}\,\{x^{p^n} - x, A'(x)\}$. For a given value of n, this power is either zero for every such polynomial, or else a positive integer, which may be thought of as arbitrarily large if the resultant happens to vanish. If the power is not zero there clearly exist polynomials of $\mathfrak{A}$ for which it assumes a minimum value. We denote this minimum by p^{q_M}, so that we shall have for some polynomial $A'(x)$ of degree N,

$$\Delta_{(n)}(A') = p^{q_M} w, \qquad (p, w) = 1, \qquad A'(x) \equiv A(x) \pmod{p},$$

while if $A''(x)$ is any other polynomial of degree N and congruent to $A(x)$ modulo p,

$$\Delta_{(n)}(A'') \equiv 0 \pmod{p^{q_M}}. \tag{2.1}$$

---

[1] This restriction will be understood in all that follows.

[2] These Annals, vol. 34, July 1933, pp. 461–479. The notation $\Delta_{(n)}(A)$ in place of the more natural $\Delta_{p^n}(A)$ is used for typographical reasons. With Lehmer's notation our $\Delta_{(n)}(A)$ would be written $(-1)^{N+1}a^N\Delta_{p^n-1}(A)$.

THEOREM 1. *The number T_M of irreducible factors $A_i(x)$ of $A(x)$ modulo p of degree M is given by the formula*

$$T_M = \frac{1}{M} \sum_{d|M} \mu(d) q_{M/d}. \tag{2.2}$$

THEOREM 2. *If p^{u_n} is the highest power of p dividing $\Delta_{(n)}(A)$, then $A(x)$ has an irreducible factor of degree M modulo p when and only when the integer*

$$s_M = \sum_{d|M} \mu(d) u_{M/d} \tag{2.3}$$

is positive.

In both theorems, $\mu(d)$ is Möbius' function, and the summation extends over all the divisors d of M.

3. As an illustration, consider the algebraically irreducible polynomial $A(x) = x^5 - 2x^3 + x^2 + 2x + 2$ for the case $p = 5$. We find by direct computation that the discriminant of $A(x)$ is congruent to 2 modulo 5, while $\Delta_{(1)}(A) \equiv 4$ modulo 5, $\Delta_{(2)}(A) \equiv 75$ modulo 125. Hence $r_1 = q_1 = 0$, $r_2 = q_2 = 2$, $T_1 = 0$, $T_2 = 1$, so that $A(x)$ has an irreducible quadratic factor (modulo 5), and no linear factors. Hence $A(x)$ must be the product of an irreducible cubic and an irreducible quadratic, (modulo 5). As a matter of fact

$$A(x) \equiv (x^2 + 2)(x^3 + x + 1) \pmod 5.$$

4. In order to prove theorems 1 and 2, we need a chain of lemmas some of which are familiar (for example lemmas 4 and 5), while others contain results of a certain arithmetical interest in themselves. In any event, none of the proofs offer any difficulties, and they are accordingly omitted here.

Let $F(x)$ be any polynomial, and p any prime such that $F(x) \not\equiv 0 \pmod p$. Denote by τ, if it exists, the least positive value of n such that

$$x^{p^n} \equiv x \quad (\text{modd } p, F(x)). \tag{4.1}$$

LEMMA 1. *$x^{p^n} \equiv x$ (modd p, $F(x)$) when and only when n is divisible by τ.*

LEMMA 2. If $x^{p^\tau} \equiv x$ (modd p, $F(x)$) *and $x^{p^\tau} - x$ is not exactly divisible by $F(x)$, so that there exists a positive integer s such that*

$$x^{p^\tau} \equiv x \quad (\text{modd } p^s, F(x)), \qquad x^{p^\tau} \not\equiv x \quad (\text{modd } p^{s+1}, F(x)),$$

then if q is any positive integer,

$$x^{p^{q\tau}} \equiv x \quad (\text{modd } p^s, F(x)), \qquad x^{p^{q\tau}} \not\equiv x \quad (\text{modd } p^{s+1}, F(x)).$$

LEMMA 3. *There exists no value of n for which*

$$x^{p^n} \equiv x \quad (\text{modd } p, F^2(x)).$$

COROLLARY 3.1. *If the polynomial $F(x)$ has a squared factor,* (4.1) *is impossible for any positive n, and any prime p.*

COROLLARY 3.2. *If the prime p divides the discriminant of $F(x)$,* (4.1) *is impossible for any positive n.*

LEMMA 4. *If $F(x)$ is irreducible, modulo p, and if*

$$\Delta_{(n)} = \Delta_{(n)}(F) = \text{Res }\{x^{p^n} - x, F(x)\},$$

then $\Delta_{(n)} \equiv 0 \pmod p$ *when and only when* $x^{p^n} - x \equiv 0$ (modd $p, F(x)$).

LEMMA 5. *If $F(x)$ is an irreducible polynomial modulo p of degree M, then the least positive value of n for which* (4.1) *is satisfied is M.*

LEMMA 6. *If $F(x)$ is an irreducible polynomial modulo p of degree M, and if k is such that*

$$x^{p^k} \equiv x \qquad \text{(modd } p^2, F(x)),$$

then one can find an indefinite number of polynomials $F'(x)$ of degree M and congruent to $F(x)$ modulo p such that

$$x^{p^k} \equiv x \quad \text{(modd } p, F'(x)), \qquad x^{p^k} \not\equiv x \quad \text{(modd } p^2, F'(x)).$$

LEMMA 7. *If $F(x)$ is an irreducible polynomial modulo p of degree M, so that by lemma* 5,

$$x^{p^M} \equiv x \qquad \text{(modd } p, F(x)),$$

and if R is any assigned positive integer, it is possible to find a polynomial $F'(x)$ of degree M and congruent to $F(x)$ modulo p such that

$$x^{p^M} \equiv x \quad \text{(modd } p^R, F'(x)), \qquad x^{p^M} \not\equiv x \quad \text{(modd } p^{R+1}, F'(x)).$$

LEMMA 8. *If $F(x)$ is an irreducible polynomial modulo p of degree M and if*

$$x^{p^k} \equiv x \quad \text{(modd } p^R, F(x)), \qquad x^{p^k} \not\equiv x \quad \text{(modd } p^{R+1}, F(x)),$$

then

$$\Delta_{(k)}(F) \equiv 0 \pmod{p^{RM}}, \qquad \Delta_{(k)}(F) \not\equiv 0 \pmod{p^{RM+1}}.$$

LEMMA 9. *If $F(x)$ is a polynomial with no repeated roots, and if p is a prime which does not divide its discriminant, there exist positive values of n for which the congruence* (4.1) *holds.*

5. Let us return now to the congruence (1.1):

$$A(x) \equiv A_1(x)A_2(x) \cdots A_r(x) \pmod p.$$

By lemmas 6, 2 and 8, we can choose each $A_i(x)$ so that if $\Delta_{(M)}(A_i) = \text{Res }\{x^{p^M} - x, A_i(x)\}$ is divisible by p, it is divisible by p^{d_i} and no higher power of p, where d_i is the degree of $A_i(x)$, and by lemmas 2, 5, and 8, $\Delta_{(M)}(A_i)$ is divisible by p when and only when d_i divides M. We may write therefore

$$\Delta_{(M)}(A_i) = p^{q_{M_i}}w_i, \qquad (p, w_i) = 1, \qquad (i = 1, 2, \cdots, r)$$

where

$$q_{M_i} = d_i \quad \text{if } d_i \text{ divides } M; \qquad q_{M_i} = 0 \quad \text{otherwise.} \tag{5.1}$$

Let the $A_i(x)$ be chosen in this manner, and let

$$A_1(x)A_2(x) \cdots A_r(x) = \bar{A}(x).$$

Then $A(x) \equiv \bar{A}(x) \pmod{p}$, and the highest power of p dividing $\Delta_{(M)}(\bar{A})$ is

$$q_M = q_{M_1} + q_{M_2} + \cdots + q_{M_r}. \tag{5.2}$$

For

$$\Delta_{(M)}(\bar{A}) = \operatorname{Res}\,\{x^{p^M} - x,\ \bar{A}(x)\} = \prod_{i=1}^{r} \operatorname{Res}\,\{x^{p^M} - x,\ A_i(x)\} = \Delta_{(M)}(A_1) \cdots \Delta_{(M)}(A_r).$$

I say that p^{q_M} is the minimal power of p dividing $\Delta_{(M)}(A')$ for all polynomials $A'(x)$ of degree N which are congruent to $A(x)$ modulo p.

For given any such polynomial, and any positive integer L, by Schönemann's second theorem,[3] there exists a decomposition of $A'(x)$ modulo p^L of the form

$$A'(x) \equiv A'_1(x)A'_2(x) \cdots A'_r(x) \pmod{p^L}$$

where $A'_i(x)$ is congruent to $A_i(x)$ modulo p, and of the same degree in x. Therefore,

$$\Delta_{(M)}(A') \equiv \Delta_{(M)}(A'_1) \cdots \Delta_{(M)}(A'_r) \pmod{p^L}.$$

If u_{M_i} is the highest power of p dividing $\Delta_{(M)}(A'_i)$, we infer that the highest power of p dividing $\Delta_{(M)}(A')$ is

$$u_M = u_{M_1} + u_{M_2} + \cdots + u_{M_r},$$

for the integer L may be chosen arbitrarily large. Since $A'_i(x)$ is congruent to $A_i(x)$ and of the same degree, $u_{M_i} \geqq q_{M_i}$ so that $u_M \geqq q_M$.

Let T_d denote the total number of irreducible factors of $A(x)$ of degree d. Then by (5.1), (5.2) may be written

$$q_M = \sum_{d|M} dT_d. \tag{5.3}$$

Our first theorem now follows immediately by applying Dedekind's inversion formula to (5.3).[4]

6. To prove our second theorem, we construct a Schönemann decomposition of $A(x)$ itself modulo p^L similar to that of $A'(x)$ in section 5, obtaining successively

$$A(x) \equiv A''_1(x)A''_2(x) \cdots A''_r(x) \pmod{p^L},$$

$$\Delta_{(M)}(A) \equiv \Delta_M(A''_1)\Delta_M(A''_2) \cdots \Delta_M(A''_r) \pmod{p^L},$$

$$u_M = u_{M_1} + u_{M_2} + \cdots + u_{M_r}, \tag{6.1}$$

[3] Fricke, *Algebra*, vol. III, Braunschweig (1928), p. 67.
[4] Landau, *Vorlesungen über Zahlentheorie*, vol. I, Leipzig (1927), p. 22.

where $A_i''(x)$ is congruent to $A_i(x)$ modulo p, and of the same degree, and u_{M_i} is now the highest power of p dividing $\Delta_M(A_r'')$.

By lemma 2, u_{M_i} is zero unless the degree of $A_i''(x)$—that is, the degree of $A_i(x)$—divides M. We may write then

$$u_M = S_M + S_M'$$

where S_M is the contribution to the right side of (6.1) of all those irreducible factors $A_i''(x)$ of $A(x)$ modulo p^L of degree M, and S_M' the contribution of all the factors whose degrees are proper divisors of M. Thus S_M is different from zero when and only when $A(x)$ has at least one irreducible factor of degree M. From lemma 2, it is clear that

$$u_M = \sum_{d|M} s_d. \tag{6.2}$$

On applying Dedekind's inversion formula to (6.2), we obtain our second theorem.

7. If the factorization of $A(x)$ modulo p is known, q_M may bc calculated by (5.3), and the minimal property of q_M gives us the congruence

$$\Delta_{(M)}(A) \equiv 0 \pmod{p^{q_M}}$$

In particular, if q_M is zero, $\Delta_{(M)}(A)$ is not divisible by p. We given in conclusion a formula for $\Delta_n(A) = \text{Res}\,\{x^n - x, A(x)\}$ which is useful in numerical applications; namely

$$\Delta_n(A) = \begin{vmatrix} W_n - W_0, & W_{n+1} - W_1, & \cdot\ \cdot & W_{n+N-1} - W_{N-1}, \\ W_{n+1} - W_1, & W_{n+2} - W_2, & \cdot\ \cdot & W_{n+N} - W_N, \\ \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot \\ \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot \\ W_{n+N-1} - W_{N-1}, & W_{n+N} - W_N, & \cdot\ \cdot & W_{n+2N-2} - W_{2N-2}, \end{vmatrix}.$$

Here (W) is that solution of the difference equation

$$\Omega_{n+N} = a_1\Omega_{n+N-1} - a_2\Omega_{n+N-2} - \cdots - a_N\Omega_n$$

associated with the polynomial $A(x)$ with the initial values $W_0 = 0$,

$$W_1 = 0, \qquad W_2 = 0, \cdots, W_{N-2} = 0, \qquad W_{N-1} = 1.$$

The essential points in the proof of this formula will be found in a paper of mine in the Transactions of the American Mathematical Society.[5]

CALIFORNIA INSTITUTE OF TECHNOLOGY.

---

[5] Vol. 35, July (1933), page 608. The element in the lower right hand corner of the determinant $\Delta(U)$ given there should read u_{2k-2} instead of u_{2k-1}, and similarly for the determinant on page 604.

ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

RATIONAL METHODS IN THE THEORY OF LIE ALGEBRAS

BY NATHAN JACOBSON

(Received May 20, 1934)

Introduction. The present note gives a development by rational methods of that part of the theory of Lie algebras (infinitesimal groups) which centers around the Lie-Engel theorems.[1] The main results are for the most part well known. The chief interest lies in the method, which consists of studying by elementary and direct means the relation between a Lie algebra and an enveloping associative algebra generated by it. The incidental machinery developed should be useful in rationalizing other parts of the theory.

My interest in this subject was aroused by the lectures of Prof. Weyl. I am indebted also to Prof. Albert for collaborating with me in the early stages of this work.

1. **Preliminaries.** We suppose that the underlying field F has characteristic 0. A *Lie algebra* over F is a linear space having a finite basis with respect to F, and having defined in it a composition of pairs of elements a, b resulting in the *commutator* $[a, b]$ such that

$$(1)\quad \alpha [a, b] = [\alpha a, b] = [a, \alpha b], \qquad [a + b, c] = [a, c] + [b, c], \qquad \alpha \in F.$$

$$(2)\quad [a, b] = -[b, a], \qquad [a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0.$$

If B and C are linear sub-spaces of L, the linear space generated by the commutators $[b, c]$, $b \in B$, $c \in C$ will be called the *commutator* of B and C, and denoted by $[B, C]$. In addition to the usual rules of calculation with linear spaces, we note, as a consequence of (2):

$$(3)\quad [B, C] = [C, B], \qquad [B, [C, D]] \subset [C, [D, B]] + [D, [B, C]].$$

B is a Lie *sub-algebra* of L if $B' = [B, B] \subset B$. B is *invariant* if $[L, B] \subset B$. The projection space L (mod B) of an invariant B is a Lie algebra. $L' = [L, L]$ is the first *derived* algebra of L, $L'' = [L', L']$ the second derived, etc. L is *solvable* if its derived sequence leads to 0, i.e. there exists an integer t such that $L^{(t)} = 0$. The n^{th} *power* of L is defined by induction as $L^n = [L, L^{n-1}]$. If $L^s = 0$, L is said to be *nilpotent*. Evidently $L^{k+1} \supset L^{(k)}$ and hence if L is nilpotent, it is solvable. A Lie algebra is *semi-simple* if it contains no solvable invariant sub-algebra other than 0. If B and C are invariant, it is easily seen that their commutator $[B, C]$ is also invariant. If S is solvable and invariant, and $S^{(t-1)} \neq 0$ while $S^{(t)} = 0$, then $S^{(t-1)}$ is an abelian invariant sub-algebra of L.

[1] For the usual proofs of the Lie-Engel theorems see H. Weyl, *Darstellung kontinuerlicher halb-einfacher Gruppen* II, Math. Zeits., **24** (1925), p. 375.

Hence we may say L is semi-simple if it contains no abelian invariant sub-algebra $\neq 0$. The sum of two solvable invariant sub-algebras is easily seen to be solvable and invariant. Thus there exist a unique maximal solvable invariant sub-algebra of L. We call it the *Lie radical* of L. If $L = L_1 + L_2$ where $L_1 \frown L_2 = 0$ and $[L_1, L_2] = 0$, then L is said to be the *direct sum* of L_1 and L_2, $L = L_1 (+) L_2$. It follows that L_1 and L_2 are invariant in L.

We recall that every Lie algebra admits a representation, the *adjoint representation*, defined by associating with every element a of L the following linear transformation of L:

$$x \to x' = [a, x] = (a)x \qquad \text{where} \qquad x \in L.$$

This is a representation in the sense that the correspondence $a \to (a)$ is linear and $[a, b] \to (a)(b) - (b)(a)$. If we have any representation of a Lie algebra, we may consider the associative algebra generated by the transformations of this representation. We are led in this way to study the following situation, of which the above is a special case: a Lie algebra L is embedded in an algebra[2] A in such a way that the commutator $[a, b]$ is realized by means of $ab - ba$ which is defined in A. (1) and (2) then follow from the postulates for an algebra. We suppose also, as we may without loss of generality, that the sub-algebra generated by multiplication and linear combination of the elements of L is the whole algebra A. A will then be called an *enveloping algebra* of L.

2. Semi-simple enveloping algebras and Lie's theorems. Let L be a Lie algebra whose enveloping algebra is A. In this section we propose to investigate the structure of L when A is semi-simple and we shall apply the results to obtain Lie's theorems. Only the most elementary facts in the theory of associative algebras will be required. Besides the definitions, we need refer only to the theorem that an algebra, all of whose elements are nilpotent, is itself nilpotent.[3] This result will be used for commutative algebras in this section, and for these a trivial direct proof may be given. In the next section, however, we require the result for arbitrary algebras.

LEMMA 1. *If M is an invariant Lie sub-algebra of L, and B and A respectively are their enveloping algebras, then AB and BA are invariant. If B is nilpotent, so are AB and BA.*

We wish to show first that

$$(4) \qquad AB \subset BA + B, \qquad\qquad BA \subset AB + B.$$

It is sufficient to show the first of these and because of the distributive law, we need to prove only that $l_1 l_2 \cdots l_s m_1 m_2 \cdots m_t \in BA + B$. Let $[l_s, m_1] = m' \in M$, then $l_s m_1 = m' + m_1 l_s$ and

[2] The term *algebra* will mean linear associative algebra with a finite basis over F in contrast with the term Lie algebra.

[3] For a proof of this theorem see J. H. Maclagan Wedderburn, *On hypercomplex numbers*, Proc. London Math. Soc., series 2, **6** (1908), p. 91 or L. E. Dickson, *Algebras and their arithmetics*, p. 46.

$$l_1 \cdots l_s m_1 \cdots m_t = l_1 \cdots l_{s-1} m' m_2 \cdots m_t + l_1 \cdots l_{s-1} m_1 l_s m_2 \cdots m_t .$$

If we use induction on s and t, we get the desired result. (4) implies that $ABA \subset AB \frown BA$ and hence AB and BA are invariant. From (4) follows also

$$(5) \qquad AB^k \subset B^k A + B^k, \qquad B^k A \subset AB^k + B^k$$

and from (5)

$$(6) \qquad (AB)^k \subset AB^k, \qquad (BA)^k \subset B^k A .$$

This equation shows that if B is nilpotent, so are AB and BA.

LEMMA 2. *If $[l, m] = m'$ is commutative with m, then m' is nilpotent.*

The operation (') defined by l has the formal properties of a derivative. It is linear and

$$(m_1 m_2)' = [l, m_1 m_2] = [l, m_1]m_2 + m_1[l, m_2] = m_1' m_2 + m_1 m_2' .$$

From the commutativity of m and m', we have $\varphi(m)' = \varphi'(m)m'$ where $\varphi(\lambda)$ is a polynomial with coefficients in F and $\varphi'(\lambda)$ is the derivative of $\varphi(\lambda)$. Now suppose $\varphi(m) = 0$. There exists such a polynomial since A has a finite basis. It follows that

$$\varphi(m) = 0, \qquad \varphi'(m)m' = 0, \cdots, \qquad \varphi^{(k)}(m)(m')^{2k-1} = 0, \cdots .$$

If the degree of $\varphi(\lambda)$ is h, then $\varphi^{(h)}(m) = h!$ and $(m')^{2h-1} = 0$.

Any associative algebra A defines a Lie algebra in which $[a, b] = ab - ba$. A is its own enveloping algebra. We use the Lie algebra notation A' for the derived algebra of A and denote the centrum of A by C.

LEMMA 3. *$C_1 = A' \frown C$ is a nilpotent algebra.*

For, if c and $c' \in C_1$, and $c' = [x, y] + [z, w] + \cdots$, then

$$cc' = [cx, y] + [cz, w] + \cdots \in A'.$$

But $cc' \in C$ also and hence C_1 is closed under multiplication. Let tr (c) be the trace of c in the regular representation of A. Since $c, c^2, c^3, \cdots \in A'$, tr $(c) =$ tr $(c^2) \cdots = 0$. Hence every element of C_1 is nilpotent and the commutative algebra C_1 is nilpotent.

LEMMA 4. *If A is semi-simple, $C_1 = A' \frown C = 0$.*

By Lemma 3, C_1 is nilpotent algebra. $AC_1 = C_1 A$ is nilpotent and invariant in A. Because of the semi-simplicity, $AC_1 = C_1 A = 0$. But then C_1 is nilpotent and invariant. Hence $C_1 = 0$.

Let S denote the Lie radical of L and A the enveloping algebra of L. In this notation we have

THEOREM 1. *If A is semi-simple, $L = S\ (+)\ L_1$ where S is abelian and L_1 is semi-simple.*

We wish to show first that $[S, L] = S^* = 0$. $S^* \subset L' \subset A'$. If S^* is $\neq 0$, it is a solvable invariant Lie sub-algebra of L and it contains $S_1 \neq 0$ an abelian invariant sub-algebra of L. (S_1 may be taken as one of the algebras of the

derived sequence of S^*.) $S_2 = [S_1, L]$ has a basis of elements of the form $s' = [s, l]$ where $s \in S$ and $l \in L$. By Lemma 2, these elements are nilpotent. Hence the commutative enveloping algebra B of S_2 is nilpotent. By Lemma 1, AB is nilpotent and invariant in A. Hence $B = 0$ and $S_2 = 0$. Thus S_1 consists exclusively of elements of the centrum. This is impossible because of Lemma 5. Hence $S^* = 0$.

On account of Lemma 4, we may obtain an L^* such that $L = S + (L' + L^*) = S + L_1$, where the spaces S, L' and L^* are independent. L_1 is a Lie algebra and $[S, L_1] = [L_1, S] = 0$. Hence $L = S\ (+)\ L_1$ q.e.d.

$L_1 \cong L - S$ is a semi-simple Lie algebra. It is a consequence of the structure theorem of Cartan that such an algebra is equal to its derived algebra. If we apply this result to L_1, we have $L_1 = L_1' \subset L'$ and hence $L_1 = L'$, $L = S\ (+)\ L'$. We shall not require this stronger form of Theorem 1 in the sequel.

The following is a generalization of a theorem of Cartan's on absolutely irreducible Lie algebras of linear transformations:[4]

THEOREM 2. *If L is a completely reducible Lie algebra of linear transformations, then L $S\ (+)\ L'$, S abelian and L' semi-simple.*

This follows directly from Theorem 1 and the proposition from general representation theory that the enveloping algebra of a completely reducible set of linear transformations is semi-simple.

The following result is fundamental for Lie's theorems on solvable Lie algebras:

THEOREM 3. *If L is solvable and N is the radical of the enveloping algebra A of L, then A (mod N) is abelian. L' is a nilpotent Lie algebra contained in N.*

If $l_1 \equiv m_1$, $l_2 \equiv m_2$ (mod N), then $[l_1, l_2] \equiv [m_1, m_2]$ (mod N). Thus the elements of L taken mod N define a Lie algebra which is isomorphic with L (not necessarily $(1 - 1)$). We denote this algebra as L (mod N). It is solvable and its enveloping algebra is A (mod N), which is semi-simple. By Theorem 1, L (mod N) is abelian and hence so is A (mod N). For any pair of elements $l_1, l_2 \in L$, $[l_1, l_2] \equiv 0$ (mod N), or $L' \subset N$. Hence L' is a nilpotent Lie algebra.

Now suppose that the elements of the solvable Lie algebra are linear transformations of a vector space $\mathfrak{R}$. In the notation of Theorem 3 we have A (mod N) is a commutative semi-simple algebra. Suppose $N^s = 0$ but $N^{s-1} \neq 0$. If B is any sub-set of A, we denote the sub-space of $\mathfrak{R}$ generated by the transforms of the vectors of $\mathfrak{R}$ by the elements of B by $B\mathfrak{R}$. Denote $N^k\mathfrak{R}$ by $\mathfrak{R}_k$. We have $\mathfrak{R}_{s+1} = 0$, $\mathfrak{R}_s \neq 0$. From the associative law, $N^{l-k}\mathfrak{R}_k = \mathfrak{R}_l$ $(l > k)$. Hence

$$\mathfrak{R} > \mathfrak{R}_1 > \mathfrak{R}_2 > \cdots > \mathfrak{R}_s > \mathfrak{R}_{s+1} = 0.$$

The spaces $\mathfrak{R}_k$ are invariant with respect to A. For,

$$A\mathfrak{R}_k = AN^k\mathfrak{R} = (AN)N^{k-1}\mathfrak{R} \subset N^k\mathfrak{R} = \mathfrak{R}_k$$

since $AN \subset N$.

[4] E. Cartan, *Les groupes de transformations etc.*, Annales de l'Ecole Normale, 3rd ser., **26** (1909), p. 148.

Consider the transformations of A in the projection space $\mathfrak{R}_k \pmod{\mathfrak{R}_{k+1}}$. If $a \equiv a' \pmod{N}$, $a, a' \in A$, then $a\mathfrak{x} \equiv a'\mathfrak{x} \pmod{\mathfrak{R}_{k+1}}$ where $\mathfrak{x} \in \mathfrak{R}_k$. Thus the representation of A determined by $\mathfrak{R}_k \pmod{\mathfrak{R}_{k+1}}$ is also a representation of $A \pmod{N}$. In particular the transformations of N are 0 in $\mathfrak{R}_k \pmod{\mathfrak{R}_{k+1}}$. Let us choose a basis for $\mathfrak{R}_s$ and supplement it to obtain a basis for $\mathfrak{R}_{s-1}$, supplement this to obtain a basis for $\mathfrak{R}_{s-2}$, etc. With respect to this basis the matrices of the transformations of A all have the form

$$(7) \qquad a = \begin{bmatrix} a_1 & a_{12} & \cdots & a_{1r} \\ & a_2 & \cdots & a_{2r} \\ & & & \cdot \\ & 0 & \cdot & \cdot \\ & & & \cdot \quad \cdot \\ & & & a_r \end{bmatrix}$$

where the a_i are the representation matrices of $A \pmod{N}$ in $\mathfrak{R}_{i-1} \pmod{\mathfrak{R}_i}$. In particular if $a \in N$, $a_1 = a_2 = \cdots a_r = 0$.

It follows from the general theory of representations of algebras that there exists a fixed algebraic field Z of finite degree over F such that any representation of the semi-simple commutative algebra $A \pmod{N}$ can be completely reduced into l-dimensional representations in Z. It follows that by choosing a suitable basis in the space obtained from $\mathfrak{R}_{i-1} \pmod{\mathfrak{R}_i}$ by extending the field to Z, the matrices a may be taken to have the form

$$(8) \qquad a_i = \begin{bmatrix} \alpha_1^{(i)} & & & 0 \\ & \alpha_2^{(i)} & & \\ & & \cdot & \\ 0 & & \cdot & \\ & & & \cdot \\ & & & \alpha_{r_i}^{(i)} \end{bmatrix}.$$

We have proved in this way the results which are essentially due to Lie:

THEOREM 4. *If L is a solvable Lie algebra of transformations, its matrices may be taken in the form* (7). *The matrices of L' then have $a_1 = a_2 = \cdots = a_r = 0$. By transforming in an algebraic field Z over F we may take the a_i to have the form* (8).

3. **Engel's theorem.** We suppose again that the elements of the Lie algebra are linear transformations of a vector space $\mathfrak{R}$. The characteristic polynomial $f(\lambda | l) = \lambda^n - \psi_1(l)\lambda^{n-1} + \psi_2(l)\lambda^{n-2} - \cdots$ of a general element l of L will be called the *characteristic polynomial of L in $\mathfrak{R}$*. In a similar fashion we define the characteristic polynomial $f(\lambda \mid a)$ of the enveloping algebra A of L. The first coefficient $\psi_1(a)$ is called the *trace* of a in $\mathfrak{R}$.

The trace of the elements of A can be computed from the characteristic polynomial of L. Since the trace is linear, one needs to compute only the trace of a single term such as $l_1 l_2 \cdots l_r$, where the $l_i \in L$. We may suppose that the trace has already been determined for terms of $(r - 1)$ factors or less. The form $\frac{1}{r!}\operatorname{tr}(\Sigma^* l_{k_1} l_{k_2} \cdots l_{k_r})$, the summation extending over all permutations of

$l_1, l_2, \cdots, l_r$, is a symmetric multilinear form associated with $\operatorname{tr}(l^r)$: If $m_1, m_2, \cdots, m_t$ is a basis for L, and $l = \lambda_1 m_1 + \lambda_2 m_2 + \cdots + \lambda_t m_t$, $l_i = \lambda_1^{(i)} m_1 + \lambda_2^{(i)} m_2 + \cdots + \lambda_t^{(i)} m_t$, and

$$\operatorname{tr}(l^r) = \frac{1}{r!} \sum \alpha_{i_1 i_2 \cdots i_r} \lambda_{i_1} \lambda_{i_2} \cdots \lambda_{i_r}$$

then

$$\frac{1}{r!} \operatorname{tr}\left(\sum{}^* l_{k_1} l_{k_2} \cdots l_{k_r}\right) = \frac{1}{r!} \sum \alpha_{i_1 i_2 \cdots i_r} \lambda_{i_1}^{(1)} \lambda_{i_2}^{(2)} \cdots \lambda_{i_r}^{(r)}$$

$\operatorname{tr}(l^r)$ can be computed from $\psi_1(l), \psi_2(l), \cdots$ and hence also the associated multilinear form can be computed. On the other hand, if $[l_{k+1}, l_k] = l'$,

$$\operatorname{tr}(l_1 \cdots l_{k-1} l_{k+1} l_k l_{k+2} \cdots l_r - l_1 l_2 \cdots l_r) = \operatorname{tr}(l_1 \cdots l_{k-1} l' l_{k+2} \cdots l_r) = \mu$$

and this involves only products of $(r - 1)$ terms and so can be computed. Since any permutation is a product of transpositions, all the terms $\operatorname{tr}(l_{k_1} \cdots l_{k_r})$ can be expressed in terms of $\operatorname{tr}(l_1 l_2 \cdots l_r)$ and traces of terms involving $(r - 1)$ factors. Hence

$$\operatorname{tr}(l_1 l_2 \cdots l_r) = \frac{1}{r!} \operatorname{tr}\left(\sum{}^* l_{k_1} l_{k_2} \cdots l_{k_r}\right) + \omega \tag{9}$$

where ω can be determined.[5]

We apply this method to obtain a generalization of Engel's theorem.

THEOREM 5. *If the characteristic polynomial of L in $\mathfrak{R}$ is λ^n, then the enveloping algebra of L is nilpotent, and L is a nilpotent Lie algebra.*

We shall show that the trace of every element of the enveloping algebra A is 0. Assume this true for elements which are linear combinations of products of $r - 1$ terms. We have $\omega = 0$ in (9). But $\operatorname{tr}(l^r) = 0$ and hence the associated form $\frac{1}{r!} \operatorname{tr}(\Sigma^* l_{k_1} \cdots l_{k_r}) = 0$. By (9) we have $\operatorname{tr}(l_1 \cdots l_r) = 0$. If a is any element of A, $\operatorname{tr}(a) = \operatorname{tr}(a^2) = \cdots = 0$, and hence a is nilpotent. By the associative algebra theorem quoted earlier, A is nilpotent. It follows that L is a nilpotent Lie algebra.

4. **Applications to abstract Lie algebras.** By means of the adjoint representation we may apply the above results to abstract Lie algebras (not necessarily contained in associative algebras).

Theorem 3 yields

THEOREM 6. *The first derived algebra of a solvable Lie algebra is nilpotent.*

The adjoint representation of the solvable Lie algebra L is a solvable Lie

---

[5] This trace argument was given by Prof. Weyl in his course on Continuous Groups, Institute for Advanced Study, Spring term 1934. It was also found by Dr. van Kampen at Hamburg, 1928, but has not been published previously.

algebra (L) of transformations. The elements of L' correspond in this representation to the elements of $(L)'$ the derived of (L). By Theorem 2 $(L)'$ is contained in an associative nilpotent algebra. Hence we have for some integer t, $(l'_1)(l'_2)\cdots(l'_t) = 0$ for arbitrary $l'_i \in (L)'$. According to the definition of the adjoint representation, if $l'_i \to (l'_i)$, then $[l'_1[l'_2[\cdots[l'_t x]\cdots] = 0$, where x is any element of L. Using this equation for $x \in L'$, we have $L'^{t+1} = 0$.

An element l of L is *nilpotent* if there exists an integer s such that the term of s brackets $[l[l[\cdots[lx]\cdots] = 0$ for any $x \in L$.

Theorem 5 becomes

THEOREM 7. *If every element of a Lie algebra L is nilpotent, then L is nilpotent.*

For if $l \to (l)$ in the adjoint representation, then

$$[l[l[\cdots[lx]\cdots] = (l)^s x = 0.$$

Hence all the transformations of the adjoint representation are nilpotent and so by Theorem 4, the enveloping algebra of the Lie algebra of this representation is nilpotent, i.e. there exists an integer t such that $(l_1)(l_2)\cdots(l_t) = 0$ for arbitrary l_i. Thus $[l_1[l_2[\cdots[l_t x]\cdots] = 0$, or $L^{t+1} = 0$.

THE INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.

ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

CONCERNING THE DIRECT PRODUCT OF ALGEBRAS

BY J. L. DORROH

(Received February 28, 1934)

Introduction. A set of elements closed under two operations, addition and multiplication, is called an algebra provided that it is an abelian group under addition and provided that multiplication is associative and both-side distributive with respect to addition.[1] It is the purpose of this paper to give a definition of the direct product of algebras which does not presuppose a basis, but which gives the ordinary direct product in case the algebras involved possess bases,[2] and to determine the conditions under which the direct product of two algebras exists.

1. **Definitions.** *If X denotes a subset of an algebra A, then $[X]$ will denote the additive group generated by the elements of X. If $x_1, x_2, \cdots, x_r$ are non-zero elements of A, they are said to be additively independent provided that $\sum_1^r m_i x_i = 0$ (m_i a rational integer) implies $m_i x_i = 0$ ($i = 1, 2, \cdots, r$), otherwise the x_i are said to be additively dependent. If for some $r > 0$, X contains r additively independent elements, but every set of $r + 1$ elements are additively dependent, then $[X]$ is said to be of rank r; $[0]$ is of rank 0.*

If A, B are subalgebras of an algebra C, the subalgebra AB of C will be said to be the primitive direct product of A and B provided that:

1.1 *$xy = yx$ for each $x \epsilon A$ and each $y \epsilon B$.*

1.2 If $x_1, x_2, \cdots, x_r; y_1, y_2, \cdots, y_s$ *denote additively independent subsets of A and B, respectively, then $[x_1y_1, x_1y_2, \cdots, y_1y_s, \cdots, x_ry_s]$ is of rank rs.*

2. **The Characteristic of an Algebra.** The condition 1.2 places a certain restriction on A and B individually. Suppose that for some $x \epsilon A$ ($x \neq 0$) and some rational integer $m > 0$, $mx = 0$. Then $my = 0$ for each $y \epsilon B$, for otherwise we have $[myx] = [ymx] = [0]$ of rank 0 contrary to 1.2. Suppose further that m is the least positive integer for which $mx = 0$, then m is prime, for if $m = pq$, $p < m$, $q < m$, it follows that for some $y \epsilon B$ $py \neq 0$ or $qy \neq 0$ since otherwise the above argument shows that $px = qx = 0$ contrary to the choice of m, but if $py \neq 0$, $qx \neq 0$ then $[pyqx] = [ypqx] = [0]$ contradicts 1.2.

DEFINITION. *An algebra such that for each of its non-zero elements x, $nx = 0$ (n a rational integer) implies $n = 0$ will be said to be of characteristic 0. An*

[1] Cf. J. H. M. Wedderburn, *Algebras which do not possess a finite basis*, Trans. Amer. Math. Soc., vol. 26 (1924).

[2] For a definition of the direct product of two algebras with finite bases, see L. E. Dickson, *Algebras and their arithmetics*, Chicago, 1923.

algebra for which there exists some prime rational integer p such that $px = 0$ *for each of its elements* x *will be said to have the characteristic* p.

What we have just shown may be stated as follows:

If AB *is the primitive direct product of* A *and* B, *then* A *has a characteristic and* B *has a characteristic which is the same as that of* A.

In §3 the following lemma will be required:

LEMMA. *If* $\bar{A}$ *is an algebra of characteristic* c, *there exists an algebra* A *of characteristic* c *which has an identity and contains a subalgebra* 1-*isomorphic to* $\bar{A}$.

Let A denote the set of all ordered pairs (n, x) where n is a rational integer and $x \epsilon \bar{A}$. Let $(n, x) + (m, x_1) = (n + m, x + x_1)$; $(n, x)(m, x_1) = (nm, nx_1 + mx + xx_1)$ and let $(n, x) = (m, x_1)$ mean $x = x_1$ and $n \equiv m \pmod{c}$. The subalgebra consisting of all elements $(0, x)$ is 1-isomorphic to $\bar{A}$ and $(1, 0)$ is the identity of A.

3. THEOREM. *If* $\bar{A}$, $\bar{B}$ *are algebras, each having the characteristic* c, *then there exists an algebra* $\bar{C}$ *which is the primitive direct product of* $\bar{A}$ *and* $\bar{B}$.

PROOF. If $\bar{A}$ contains an identity let $\bar{A} = A$; otherwise let A denote an algebra of characteristic c which contains $\bar{A}$ and has an identity. Let B denote an algebra similarly defined with respect to $\bar{B}$. Let C denote the set of all expressions $\sum_{i=1}^{m} (x_i, y_i)$ for every rational integer $m > 0$, where x_i and y_i range independently over A and B, respectively. Then, by definition, C is closed under addition. Let

$$\left\{\sum_{i=1}^{m} (x_i, y_i)\right\}\left\{\sum_{j=1}^{n} (x'_j, y'_j)\right\} = \sum_{i,j=1}^{\substack{i=m\\ j=n}} (x_i x'_j, y_i y'_j)$$

so that C is closed under multiplication and multiplication in C is associative.

If $\xi = \sum_{i=1}^{m} (x_i, y_i)$ and $\bar{y}_1, \bar{y}_2, \cdots, \bar{y}_r$ are additively independent elements of B such that[3] $[\bar{y}_1, \bar{y}_2, \cdots, \bar{y}_r] \supseteq [y_1, y_2, \cdots, y_m]$ so that[4] $y_i = \sum_k a_{ik}\bar{y}_k$, $1 \leqq i \leqq m$, then $\sum_{k=1}^{r} (\sum_{i=1}^{m} a_{ik}x_i, \bar{y}_k)$ will be called the expression of ξ in terms of $\bar{y}_1, \bar{y}_2, \cdots, \bar{y}_r$. Consider a second element $\eta = \sum_{j=1}^{n} (x'_j, y'_j)$ of C, we may suppose that $[y'_1, y'_2, \cdots, y'_n]$ also lies in $[\bar{y}_1, \bar{y}_2, \cdots, \bar{y}_r]$, and let $z_1, z_2, \cdots, z_s$ denote a second additively independent subset of B and such that $[z_1, z_2, \cdots, z_s] \supseteq [\bar{y}_1, \bar{y}_2, \cdots, \bar{y}_r]$, then ξ and η have the same expression in terms of the z_i if, and only if, they have the same expression in terms of the $\bar{y}_i$. Let $\bar{y}_k = \sum_p \alpha_{kp} z_p$ so that if $\sum_{k=1}^{r} (\sum_{j=1}^{n} b_{jk}x'_j, \bar{y}_k)$ is the expression of η in terms of the $\bar{y}_k$, then $\sum_{p=1}^{s} (\sum_{i,k} a_{ik}\alpha_{kp}x_i, z_p)$ and $\sum_{p=1}^{s} (\sum_{j,k} b_{jk}\alpha_{kp}x'_j, z_p)$ are the expressions in terms of the z_p for ξ and η, respectively. If ξ and η have the same expression in terms of the $\bar{y}_k$, then $\sum_i a_{ik}x_i = \sum_j b_{jk}x'_j$ $(k = 1, 2, \cdots, r)$; multiplying both members of this equation by α_{kp} and summing with respect to k we have

[3] That such an independent set exists is a consequence of the fundamental theorem on abelian groups. For a proof of this theorem, see B. L. van der Waerden, *Moderne Algebra*, vol. 2, Berlin, 1931, p. 126.

[4] The a_{ik} are rational integers.

$\sum_{i,k} a_{ik}\alpha_{kp}x_i = \sum_{j,k} b_{ik}\alpha_{kp}x'_j$, $p = 1, 2, \cdots, s$; *i.e.* ξ and η have the same expression in terms of the z_p. Since the $\bar{y}_k$ are independent, the array of the α's contains an r-columned minor whose determinant is not congruent to zero (mod. c) (c is the characteristic of A and B). Let α denote this minor. If we assume $\sum_{i,k} a_{ik}\alpha_{kp}x_i = \sum_{j,k} b_{jk}\alpha_{kp}x'_j$ for $1 \leqq p \leqq s$ and write $\bar{x}_k = \sum_i a_{ik}x_i - \sum_j b_{jk}x'_j$ $(k = 1, 2, \cdots, r)$ we have in vector notation

$$\alpha'(\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_r) = 0;$$

multiplying on the left by (adj. α)$'$ we obtain

$$|\alpha|(\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_r) = 0$$

and since $|\alpha| \not\equiv 0$ (mod. c), $\bar{x}_k = 0$, $k = 1, 2, \cdots, r$ so that ξ and η have the same expressions in terms of the $\bar{y}_k$.

Corollary. *If $\xi, \eta \in C$, Z and Y additively independent subsets of B in terms of each of which ξ and η are expressible, ξ and η have the same expression in terms of Z if they have the same expression in terms of Y.*

If $\xi, \eta \in C$, $\xi = \eta$ will mean that ξ and η have the same expression in terms of an additively independent subset of B. With this definition of equality between elements of C it follows that addition in C is commutative and that C contains a zero element $(0, y) = (x, 0)$ and the negative of each of its elements. Furthermore, if $\xi_1 = \xi_2$, $\xi_3 = \xi_4$, then $\xi_1 + \xi_3 = \xi_2 + \xi_4$ and $\xi_1\xi_3 = \xi_2\xi_4$ so that sums and products in C are independent of the manner of expressing the respective summands and factors. That these last assertions are valid can be seen by observing that sums and products in C are unaltered when each summand or factor is replaced by its equivalent expression in terms of some additively independent subset of B. This completes the conditions that C be an algebra.

The subalgebra A_1 consisting of all elements $(x, 1)$, $x \in A$ is 1-isomorphic to A, the subalgebra B_1 consisting of all elements $(1, y)$, $y \in B$ is 1-isomorphic to B and C is the primitive direct product of A_1 and B_1. If we denote by $\bar{A}_1$ and $\bar{B}_1$ the sets $(\bar{x}, 1)$, $\bar{x} \in \bar{A}$ and $(1, \bar{y})$, $\bar{y} \in \bar{B}$, respectively, then $\bar{C} = \bar{A}_1\bar{B}_1$ is the primitive direct product of $\bar{A}_1$ and $\bar{A}_1$ and $\bar{A}_1$, $\bar{B}_1$ are 1-isomorphic to $\bar{A}$ and $\bar{B}$, respectively.

4. **Relative Direct Products.** If with an algebra A there is associated a field F so that $ax = xa \in A$ if $x \in A$ and $a \in F$, and $a(bx) = (ab)x$; $1x = x$; $a(x + y) = ax + ay$; $(a + b)x = ax + bx$; $a(xy) = (ax)y = x(ay)$, then A is said to be an algebra over the field F.

Definition. *If A, B are algebras over a field F and if C is an algebra containing both A and B, the subalgebra AB of C is called the direct product of A and B relative to F provided that:*

4.1 $xy = yx$ *if* $x \in A$ *and* $y \in B$.

4.2 If $x_1, x_2, \cdots, x_r$ *are elements of A linearly independent with respect to F,*

and $y_1, y_2, \cdots, y_s$ are elements of B linearly independent with respect to F, then $x_1y_1, x_1y_2, \cdots, x_1y_s, \cdots, x_ry_s$ are linearly independent with respect to F.

THEOREM. *If A, B are algebras over a field F, there exists an algebra C which is the direct product of A and B relative to F.*

To prove this theorem we need only modify the argument in §3 by replacing additive independence by linear independence with respect to F.

THE JOHNS HOPKINS UNIVERSITY.

Annals of Mathematics
Vol. 36, No. 4, October, 1935

INVOLUTORIAL SIMPLE ALGEBRAS AND REAL RIEMANN MATRICES[1]

By A. Adrian Albert

(Received April 17, 1935)

Introduction

1. **A Hilbert Irreducibility theorem.** Any algebraic theory depends in part on the properties of its reference field $\mathfrak{K}$. In particular it is generally desirable to know whether or not the Hilbert Irreducibility theorem holds in $\mathfrak{K}$.

W. Franz studied[2] fields with this question in mind and proved that $\mathfrak{K}$ is a Hilbert Irreducibility field if it is a separable algebraic extension of finite degree over a Hilbert Irreducibility field $\mathfrak{F}$. This is however insufficient for the theory of algebras over a modular field since the field $\mathfrak{K}$ may be inseparable[3] over $\mathfrak{F}$.

We shall treat this latter case here and shall show that any algebraic extension $\mathfrak{K}$ of finite degree over a Hilbert Irreducibility field $\mathfrak{F}$ is a Hilbert irreducibility field. Moreover this result will be a sufficiently good tool for the researches of later chapters.

2. **Involutorial simple algebras.** The algebra $\mathfrak{M}$ of all n-rowed square matrices with elements in the field $\mathfrak{C}$ of all complex numbers is the most elementary example of an involutorial simple algebra. If we let each matrix A of $\mathfrak{M}$ correspond to its transpose $A^J = A'$ the correspondence J is an involution of $\mathfrak{M}$ in which the elements of its centrum $\mathfrak{C}$ are self corresponding, and $\mathfrak{M}$ is J-involutorial of the first kind. Moreover $\mathfrak{M}$ is J-involutorial of the second kind under the correspondence $A^J = \bar{A}'$ so that $\mathfrak{C} = \mathfrak{R}(i)$, $i^J = \bar{\imath} = -i$, $r^J = r$ for every real r.

A more complicated special case is that of the multiplication algebra $\mathfrak{D}$ of any pure Riemann matrix. C. Rosati[4] discovered the involutorial character of the division algebra $\mathfrak{D}$ and thus obtained some of the elementary properties of J-involutorial division algebras.[5] Subsequently the author[6] completely determined the structure of $\mathfrak{D}$ but his proof contained some highly undesirable complications due to the fact the necessary elementary properties of J-involutorial simple algebras had never been studied. This is but an instance of the more general observation that *we may best study the properties of a division algebra* $\mathfrak{D}$

[1] Presented to the Society, November 30, 1934.
[2] See the Table of Literature.
[3] Cf. Van der Waerden (1), vol. I, p. 113, for definitions.
[4] Rosati (1), (2), (3).
[5] Rosati (3).
[6] Albert (1), (3), (5).

by studying the class of all simple algebras $\mathfrak{M} \times \mathfrak{D}$. Let us then consider J-involutorial simple algebras $\mathfrak{A}$ over $\mathfrak{F}$.

The above example of matrices with complex elements shows that the same algebra $\mathfrak{A}$ may have entirely different involutions if the involutions of the centrum $\mathfrak{K}$ of $\mathfrak{A}$ are permitted to vary. Since these latter involutions are trivially determined[7] it is sufficient to consider only involutions T in which $k^T = k^J$ for every k of $\mathfrak{K}$. We shall do this[7] and shall prove that every such T is obtained by transformation

$$a \leftrightarrow a^T = pa^Jp^{-1}$$

by a regular quantity $p = \pm p^J$ of $\mathfrak{A}$.

Any simple algebra $\mathfrak{A}$ over $\mathfrak{F}$ is the direct product[8] of a total matric algebra $\mathfrak{M}$ by a division algebra $\mathfrak{D}$ whose centrum $\mathfrak{K}$ is the centrum of $\mathfrak{A}$. If $\mathfrak{D}$ is J-involutorial then so is $\mathfrak{K}$ and the algebra $\mathfrak{M}$ may be thought of as an algebra of matrices

$$A = (a_{ij}) \qquad (a_{ij} \text{ in } \mathfrak{K})$$

Thus $\mathfrak{M}$ is J-involutorial under the correspondence $A \leftrightarrow A^J = (b_{ij}),\ b_{ij} = a_{ji}^J$, so that A^J is the J-transpose of A. Hence $\mathfrak{M} \times \mathfrak{D} = \mathfrak{A}$ is also involutorial. Conversely we shall prove[7] that if $\mathfrak{A}$ is J-involutorial over $\mathfrak{F}$ we may choose a J-centrum preserving involution J of $\mathfrak{A}$ such that if A is in $\mathfrak{M}$ then A^J is the J-transpose of A, and such that $\mathfrak{D}$ is J-involutorial. This result thus reduces the study of $\mathfrak{D}$ to any desired $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$, and hence to the study of J-involutorial crossed products.[9]

We shall obtain complete necessary and sufficient conditions that a given division algebra $\mathfrak{D}$ *shall be J-involutorial.* In particular we shall prove that $\mathfrak{D}$ is *J-involutorial of the first kind if and only if it has exponent two.* Finally we shall study the case where $\mathfrak{F}$ is algebraic of finite degree over the field of rational numbers and then obtain a much simpler determination of the multiplication algebras of pure Riemann matrices than that referred to above.[10]

3. **The matrices of Weyl.** Let ω be a Riemann matrix[11] of genus p over a real field $\mathfrak{F}$ so that

$$\Omega = \begin{pmatrix} \omega \\ \bar{\omega} \end{pmatrix}$$

is non-singular. If C is a principal matrix[11] of ω and

$$R_\omega = i\Omega^{-1}\begin{pmatrix} I_p & 0 \\ 0 & -I_p \end{pmatrix}\Omega, \qquad R_\omega^2 = -I_{2p},$$

[7] See Chapter II.
[8] Wedderburn (1), (3).
[9] Cf. Hasse (2).
[10] In particular in Albert (5).
[11] Cf. Scorza (2), (3), Lefschetz (1), (4), Albert (1) for definitions.

then R_ω is a real matrix and $R_\omega C$ is positive definite. H. Weyl considered[12] such matrices R and generalized the concept by dropping the assumption $R^2 = -I_p$.[13] He also showed that the reduction theory for his more general matrices is obtainable exactly as for Riemann matrices.

The generalization of Weyl is seen to be insufficient when the multiplication algebra of an irreducible R of Weyl is studied. This was also true of Riemann matrices where it was necessary to introduce the concept of *Omega matrices*.[14]

We shall generalize[15] Weyl's definition to matrices with elements in an algebraically closed J-involutorial field and shall then reduce the considerations made to the following most interesting case.

Let Γ_0 be a real closed (non-modular)[16] field, $\Gamma = \Gamma_0(i)$, $i^2 = -1$. Then Γ is algebraically closed and we write $\alpha = \alpha_1 + \alpha_2 i$, $\bar{\alpha} = \alpha_1 - \alpha_2 i$ for every α of Γ, α_1 and α_2 of Γ_0. Assume that $\mathfrak{F}$ is a proper sub-field of Γ and that $\bar{a}$ is in $\mathfrak{F}$ for every a of $\mathfrak{F}$. A p-rowed square matrix R with elements in Γ will be called a Weyl matrix over $\mathfrak{F}$ if there exists a matrix $C = \pm \bar{C}'$ with elements in $\mathfrak{F}$ such that $\tau = RC$ is Hermitian. We consider isomorphic Weyl matrices and their multiplication algebras $\mathfrak{A}$ and again reduce the study of $\mathfrak{A}$ to the case where R is irreducible, $\mathfrak{A} = \mathfrak{D}$ is a division algebra.

The multiplication algebra $\mathfrak{D}$ of R is J-involutorial over $\mathfrak{F}$ and $a^J = \bar{a}$ for every a of $\mathfrak{F}$. But J is not arbitrary in $\mathfrak{D}$ since if $A = A^J$ is in $\mathfrak{D}$ the characteristic roots of A must be real, that is in Γ_0. This result was first discovered by Rosati[17] for the case of Riemann matrices and the author proved a partial converse.[18] We shall prove this same converse for Weyl matrices R and shall obtain a complete set of necessary and sufficient conditions that a J-involutorial division algebra $\mathfrak{D}$ (previously studied) may be the multiplication algebra of a Weyl matrix R.

4. **The $\mathfrak{F}$-algebra of a Weyl matrix.** The $\mathfrak{F}$-algebra $\mathfrak{B}$ of a Weyl matrix R is the set of all matrices A with elements in $\mathfrak{F}$ such that $R^{-1}AR = B$ has elements in $\mathfrak{F}$. Two Weyl matrices R and S are *associated* in $\mathfrak{F}$ if $S = GRH$ where G and H have elements in $\mathfrak{F}$ and are non-singular. Algebra $\mathfrak{B}$ contains the multiplication algebra $\mathfrak{A}$ of R and we call R a central Weyl matrix[19] if $\mathfrak{B} = \mathfrak{A}$, and shall prove that every Weyl matrix is *associated with a central Weyl matrix*. We shall also obtain a theory of the reduction of a central Weyl matrix to irreducible central components. This theory is of great importance for the theory of real Riemann matrices.

---

[12] Weyl (1).

[13] We shall use the notation I_r to represent the r-rowed identity matrix throughout this memoir.

[14] Albert (1). See also Chapter V.

[15] Chapter III.

[16] Artin-Schreier (1), (2).

[17] Cf. Rosati (3).

[18] Albert (1).

[19] In Chapter IV.

5. **The matrix R^{-1}.** If R is an *irreducible central Weyl matrix* then so is R^{-1}. Let $R^{-1} = GHR$ be associated with R and let $\mathfrak{D}$ be the multiplication algebra of R. Then we shall study[18] the properties of the linear set $\mathfrak{A}$ of quantities

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_1 \end{pmatrix} + \begin{pmatrix} A_2 & 0 \\ 0 & A_2 \end{pmatrix}\begin{pmatrix} 0 & H \\ -G & 0 \end{pmatrix},$$

where A_1 and A_2 range independently over all quantities of $\mathfrak{D}$. This set is a linear associative algebra and, when R is real and $\mathfrak{F}$ is real, algebra $\mathfrak{A}$ is the multiplication algebra of the real Riemann matrix (R, iI_p) over $\mathfrak{F}$.

6. **Omega matrices over $\mathfrak{F}$.** Let R be a Weyl matrix over $\mathfrak{F}$ with principal matrix $C = \pm\bar{C}'$ so that, if $i_0 = 1$ or i, the matrix $C_0 = i_0 C$ is Hermitian. Then we shall prove that $R^2 = \pm I_p$ if and only if $R_0 = i_0^{-1}R$ has the property $R_0^2 = I_p$. Thus $R_0 = \Omega^{-1}Er\Omega$, where Ω is a non-singular matrix with elements in Γ and

$$E_r = \begin{pmatrix} I_r & 0 \\ 0 & -I_{p-r} \end{pmatrix}, \qquad R = R_\Omega = i_0\,\Omega^{-1}E_r\Omega.$$

Moreover we shall prove that Ω is an Omega matrix of index r over $\mathfrak{F}$ and has the same multiplication algebra as R. We shall also show that if p is sufficiently large then the earlier necessary and sufficient conditions on $\mathfrak{D}$ are still valid.

7. **Real Riemann matrices.** The first systematic study of real algebraic varieties was made by F. Klein[20] and later amplified by A. Comessatti.[21] S. Lefschetz studied real abelian varieties[22] and proved that the corresponding Riemann matrices could be put into the canonical form

$$(\omega_1, \omega_2 i),$$

where ω_1 and ω_2 are real p-rowed square matrices. Cherubino later proved[23] that a Riemann matrix ω is the Riemann matrix of a real abelian variety if and only if $\alpha\omega = \bar{\omega}A$ for a rational matrix A with $A^2 = I_{2p}$. He then obtained a canonical form which may easily be derived from that of Lefschetz.

Lefschetz, Comessatti and Cherubino obtained numerous further results[24] but their theorems are mainly concerned with the properties of the abelian variety and do not solve the fundamental questions (already solved for general Riemann matrices) on the structure of real Riemann matrices.

We shall consider real Riemann matrices ω over a real field $\mathfrak{F}$ and shall prove

[20] Klein (1), (2).

[21] Comessatti (1).

[22] Lefschetz (2), (3).

[23] Cherubino (1).

[24] Lefschetz (2), (3), Cherubino (1), (2), Comessatti (1), (2), (3), as well as further papers which are listed in Lefschetz (4).

that every such matrix is isomorphic to $\omega = (R, iI_p)$ where R is a real central matrix. Conversely every (R, iI_p) is a real Riemann matrix. The reduction of R to irreducible central components R_j provides a reduction of ω to *irreducible components* $\omega_j = (R_j, iI_p)$. If R is irreducible and not associated with R^{-1} then $\omega = (R, iI_p)$ is pure and has its multiplication algebra equivalent to that of R. If R is irreducible and is associated with R^{-1} then the multiplication algebra of (R, iI_p) is the algebra $\mathfrak{A}$ of Section 6 and ω *is either pure or isomorphic to*

$$\begin{pmatrix} \omega_1 & 0 \\ 0 & \bar{\omega}_1 \end{pmatrix},$$

where ω_1 *is pure and not real.* These results completely determine the structure of any real Riemann matrix and we shall prove the existence of pure real Riemann matrices of the various types and with given multiplication algebras.

I. A Hilbert Irreducibility Theorem

1. **The theory of Hilbert and Franz.** A field $\mathfrak{K}$ is called a Hilbert Irreducibility field (H.I. field) if the following theorem is true in $\mathfrak{K}$:

Hilbert Irreducibility Theorem. *Let*

$$f(x_1, \cdots, x_r; t_1, \cdots, t_s) \equiv \prod_{i=1}^{\mu} f_i(x_1, \cdots, x_r; t_1, \cdots t_s) \tag{1}$$

be a decomposition into factors irreducible in $\mathfrak{K}(t_1, \cdots t_s)$ *of a polynomial* $f(x_1, \cdots, t_s)$ *with coefficients in* $\mathfrak{K}$. *Then there exist infinitely many sets of quantities* $\bar{t}_1, \cdots, \bar{t}_s$ *in* $\mathfrak{K}$ *such that the* $f_i(x_1, \cdots, x_r; \bar{t}_1, \cdots, \bar{t}_s)$ *are irreducible in* $\mathfrak{K}$.

Hilbert proved[25] that the field $\mathfrak{R}$ of all rational numbers is an H.I. field. He also showed that any finite algebraic extension $\mathfrak{K}$ of $\mathfrak{R}$ is an H.I. field and that the H.I. theorem holds in $\mathfrak{K}$ for $\bar{t}_1, \cdots, \bar{t}_s$ in $\mathfrak{R}$. An analogous result was proved by W. Franz[25] who obtained

Theorem F1. *Every separable algebraic extension* $\mathfrak{K}$ *of finite degree over an H.I. field* $\mathfrak{F}$ *is an H.I. field and the H.I. theorem holds in* $\mathfrak{K}$ *for* $\bar{t}_1, \cdots, \bar{t}_s$ *in* $\mathfrak{F}$.

Franz also proved

Theorem F2. *Let* $\mathfrak{F} = \Omega(\xi)$ *where* ξ *is an indeterminate and* Ω *is any infinite field. Then* $\mathfrak{F}$ *is an H.I. field.*

Theorem F3. *A field* $\mathfrak{K}$ *is an H.I. field if and only if the H.I. theorem holds in* $\mathfrak{K}$ *for polynomials in* x *and* t

$$f_i(x, t) \equiv x^{n_i} + a_{i1}(t)x^{n_i-1} + \cdots + a_{n_i}(t) \qquad (i = 1, \cdots, \mu), \tag{2}$$

with coefficients in $\mathfrak{K}$.

The case where $\mathfrak{K}$ is an inseparable extension of an H.I. field $\mathfrak{F}$ was left open by Franz and it seems not to have been treated as yet. We shall prove

[25] See the Table of Literature.

THEOREM 1. *Every algebraic extension $\mathfrak{K}$ of finite degree of an H.I. field $\mathfrak{F}$ is an H.I. field.*[26]

2. **Reduction to primitive inseparable fields.**[27] We may call a field $\mathfrak{K}$ primitive over $\mathfrak{F}$ if there exists no field $\mathfrak{K}_0$ such that $\mathfrak{K} > \mathfrak{K}_0 > \mathfrak{F}$. If z is in a primitive field $\mathfrak{K}$ over $\mathfrak{F}$ and not in $\mathfrak{F}$ then $\mathfrak{K} \geqq \mathfrak{F}(z) > \mathfrak{F}$, so that $\mathfrak{K} = \mathfrak{F}(z)$ is a simple extension of $\mathfrak{F}$. An inseparable primitive extension $\mathfrak{K}$ of finite degree over $\mathfrak{F}$ of characteristic p is a field $\mathfrak{F}(z)$ such that $z^{pn} + b_1 z^{p(n-1)} + \cdots + b_n = 0$. Then $\mathfrak{K} > \mathfrak{F}(z^p) \geqq \mathfrak{F}$ so that $z^p = a$ is in $\mathfrak{F}$. A trivial induction then gives

LEMMA 1. *Let $\mathfrak{K}$ be algebraic of finite degree over $\mathfrak{F}$. Then*

$$\mathfrak{F} = \mathfrak{K}_0 < \mathfrak{K}_1 < \cdots < \mathfrak{K}_\rho = \mathfrak{K}, \qquad \mathfrak{K}_j = \mathfrak{K}_{j-1}(z_j),$$

where each $\mathfrak{K}_j$ is primitive over $\mathfrak{K}_{j-1}$, and if $\mathfrak{K}_j$ is inseparable then $\mathfrak{F}$ has characteristic p, and $z_j^p = a_j$ in $\mathfrak{K}_{j-1}$.

Assume as the basis of an induction on j that the H.I. theorem holds in $\mathfrak{K}_{j-1}$. If $\mathfrak{K}_j$ is a separable extension of $\mathfrak{K}_{j-1}$ then the H.I. theorem holds in $\mathfrak{K}_j$ by Theorem F1. *Hence we have reduced our proof of Theorem* 1 *to a consideration of the case where $\mathfrak{F}$ has characteristic p and $\mathfrak{K} = \mathfrak{F}(z)$, $z^p = a$ in $\mathfrak{K}$.* We restrict all further discussion to this case.

3. **Two types of polynomials.** Let

$$f(x, t) \equiv a_0 x^n + a_1 x^{n-1} + \cdots + a_n, \qquad a_0 = 1\,, \tag{3}$$

be a polynomial in x and t with coefficients in $\mathfrak{K}$ and irreducible in $\mathfrak{K}(t)$. We then have

LEMMA 2. *There exists an α in $\mathfrak{K}$ such that $f(\alpha, t)$ is not in $\mathfrak{F}(t)$ if and only if $f(x, t)$ does not have the form*

$$f(x, t) = \sum_{j=0}^{\nu} b_j(t) x^{jp}, \qquad b_j(t) \text{ in } \mathfrak{F}(t). \tag{4}$$

For α^p is in $\mathfrak{F}$ for every α of $\mathfrak{K}$ and if $f(x, t)$ has the form (4) then $f(\alpha, t)$ is obviously in $\mathfrak{F}(t)$. Conversely let $f(x, t)$ not have the form (4) and suppose first that at least one a_i is not in $\mathfrak{F}(t)$. Expand $f(x, t)$ as a polynomial in z. Then there exists an i such that $0 < i < p$ and the coefficient $P(x, t)$ of z^i in $f(x, t)$ is not identically zero. The field $\mathfrak{F}$ is infinite and hence there exists an α in $\mathfrak{F}$ such that $P(\alpha, t) \neq 0$. Then $f(\alpha, t)$ is not in $\mathfrak{F}(t)$. There remains the case where all the a_i are in $\mathfrak{F}(t)$ and at least one $a_i \neq 0$ for $n - i = pq_i + r_i$, $0 < r_i < p$. Then $f(\lambda z, t) = \sum_j a_j \lambda^j a^{q_j} z^{r_j}$ and the term of degree i in λ of the coefficient of z^{r_i} is $a_i \lambda^i a^{q_i} \neq 0$. By proper choice of λ_0 in $\mathfrak{F}$ we make the total coefficient not zero and $f(\lambda_0 z, t)$ not in $\mathfrak{F}(t)$. This proves Lemma 2 and we now obtain

[26] We shall actually prove that we may transform our polynomials $f_i(x, t)$ by a linear transformation on x so that the $\bar{t}$ may be taken in $\mathfrak{F}$. However it seems probable that $f(x, t)$ may have such a form that $\bar{t}$ *must* be in $\mathfrak{K}$ if we *do not* transform $f(x, t)$.

[27] Cf. Van der Waerden, vol. I, p. 113 for definitions.

LEMMA 3. *Let $f(x, t)$ not have the form* (4). *Then there exists a polynomial*

$$F(x, t) = x^{np} + A_1 x^{(n-1)p} + \cdots + A_n \qquad (A_i \textit{ in } \mathfrak{F}(t)),$$

irreducible in $\mathfrak{F}(t)$ and such that whenever $\bar{t}$ is in $\mathfrak{F}$ and $F(x, \bar{t})$ is irreducible in $\mathfrak{F}$ then $f(x, \bar{t})$ is irreducible in K.

For we choose α as in Lemma 2 and let

$$(5) \qquad g(x, t) = f(x + \alpha, t) = x^n + c_1 x^{n-1} + \cdots + c_n,$$

where $c_n = f(\alpha, t)$ is not in $\mathfrak{F}(t)$. Write $F(x, t) = [g(x, t)]^p$. Then $F(x, t)$ has coefficients in $\mathfrak{F}$ and we may write $F(x, t) = G(x, t) \cdot H(x, t)$, where $G(x, t)$ is a polynomial in x with coefficients in $\mathfrak{F}(t)$, leading coefficient unity, and irreducible in $\mathfrak{F}(t)$. The factors of $G(x, t)$ irreducible in $\mathfrak{K}(t)$ are factors of $F(x, t)$ and hence must coincide with $g(x, t)$. By comparing leading coefficients we have $G(x, t) = | g(x, t) |^\pi$ with $\pi \leqq p$. The constant term of $G(x, t)$ is c_n^π which is in $\mathfrak{F}(t)$. There exists a $\bar{t}$ in $\mathfrak{F}$ such that $\gamma_n = c_n(\bar{t})$ is in $\mathfrak{K}$ and not in $\mathfrak{F}$, so that $\mathfrak{K} = \mathfrak{F}(\gamma_n)$. But γ_n^π is in $\mathfrak{F}$ so that $\pi = p$ and $F(x, t)$ is irreducible in $\mathfrak{F}(t)$. We now let $\bar{t}$ be in $\mathfrak{F}$ and $F(x, \bar{t})$ be irreducible in $\mathfrak{F}$. If $g(x, \bar{t}) = h(x) \cdot d(x)$ where $h(x)$ is not constant and is irreducible in $\mathfrak{K}$ then $F(x, \bar{t}) = [h(x)]^p \cdot [d(x)]^p = H(x) \cdot D(x)$ where $H(x)$ and $D(x)$ have coefficients in $\mathfrak{F}$. Then $D(x)$ is constant so that so is $d(x)$ and $g(x, \bar{t})$ is irreducible in $\mathfrak{K}$. But $g(x, \bar{t}) = f(x + \alpha, \bar{t}) = f(y, \bar{t})$ is irreducible in $\mathfrak{K}$ and so is $f(x, \bar{t})$.

There remains the more troublesome case of polynomials of the form (4). For this case we may prove

LEMMA 4. *Let*

$$(6) \qquad d(t) = \beta_0 + \beta_1 t^p + \cdots + \beta_m t^{mp} \qquad (\beta_i \textit{ in } \mathfrak{F}),$$

be not the p^{th} power of a quantity of $\mathfrak{K}(t)$. Then there exist at most m distinct quantities $\bar{t}_i$ of $\mathfrak{F}$ such that $d(\bar{t}_i) = \lambda_i^p$ with λ_i in $\mathfrak{K}$.

For if $d_1 = \lambda_1^p$ and $d_2 = \lambda_2^p$ then $d_1 + d_2 = (\lambda_1 + \lambda_2)^p$ in a field $\mathfrak{K}$ of characteristic p. We assume that $d(\bar{t}_i) = \lambda_i^p$ with λ_i in $\mathfrak{K}$ for $i = 1, \cdots, m$ and write $t_1 = t - \bar{t}_1$,

$$(7) \qquad d(t) = \sum_{i=0}^{m} \beta_i (t_1 + \bar{t}_1)^{pi} = \sum_{i=0}^{m} \beta_i (t_1^p + \bar{t}_1^p)^i = d(\bar{t}_1) + t_1^p \, d_1(t_1),$$

where

$$(8) \qquad d_1(t_1) = \beta_{01} + \beta_{11} t_1^p + \cdots + \beta_{m-1,1} \, t_1^{(m-1)p} \qquad (\beta_{j}, \text{ in } \mathfrak{F}).$$

But $d(\bar{t}_1) = \lambda_1^p$ and $d(\bar{t}_2) = \lambda_1^p + (\bar{t}_2 - \bar{t}_1)^p \, d_1(\bar{t}_2 - \bar{t}_1) = \lambda_2^p$ with $\bar{t}_2 \neq \bar{t}_1$. Hence $d_1(\bar{t}_2 - \bar{t}_1) = \lambda_{20}^p$ with

$$\lambda_{20} = (\lambda_2 - \lambda_1) \, (\bar{t}_2 - \bar{t}_1)^{-1}$$

in $\mathfrak{K}$. By the above proof $d_1(t_1) = \lambda_{20}^p + d_2(t_2) t_2^p$, where $t_2 = t_1 - (\bar{t}_2 - \bar{t}_1) = t - \bar{t}_2$ and $d_2(t_2)$ has degree $m - 2$ in t_2^p. A repeated application of this process evidently yields

$$d(t) = [h(t)]^p + \delta[(t - \bar{t}_1) \cdots (t - \bar{t}_n)]^p,$$

where $h(t)$ has coefficients in $\mathfrak{K}$ but δ is in $\mathfrak{F}$. If $\delta = \lambda^p$ for λ in $\mathfrak{K}$ then $d(t) = [h(t) + \lambda(t - \bar{t}_1) \cdots (t - \bar{t}_n)]^p$, a contradiction. Then if $\bar{t} \neq \bar{t}_i$ is in $\mathfrak{F}$ and $(\bar{t} - \bar{t}_1) \cdots (\bar{t} - \bar{t}_n) = \tau \neq 0$ we have

$$d(\bar{t}) = [h(t)]^p + \delta\, \tau^p \neq \lambda^p$$

with λ in $\mathfrak{K}$, since otherwise $\delta = \tau^{-p}\,[\lambda - h(\bar{t})]^p$, a contradiction.

We now have

LEMMA 5. *Let $f(x, t)$ have the form (4) with*

$$b_j = B_j(t^p)\ , \tag{9}$$

and let T be the set of all quantities $\bar{t}$ in $\mathfrak{F}$ for which $f(x, \bar{t})$ is irreducible in $\mathfrak{F}$. Then $f(x, \bar{t})$ is irreducible in $\mathfrak{K}$ for all but a finite number of quantities of T.

For if all the $B_j(t^p) = [A_j(t)]^p$ where $A_j(t)$ has coefficients in $\mathfrak{K}$ then obviously

$$f(x, t) \equiv \left[\sum_{j=0}^{\nu} A_j(t)x^j\right]^p$$

contrary to our hypothesis that $f(x, t)$ is irreducible in $\mathfrak{K}(t)$. We may then assume that in particular $b_i(t) \not\equiv [A_i(t)]^p$. By Lemma 4 we omit a finite number of quantities from T and obtain a new set T_0 such that for every $\bar{t}$ of T_0 we have $b_i(\bar{t}) \neq \lambda^p$ for any λ of $\mathfrak{K}$. Then obviously $f(x, \bar{t}) \neq [g(x)]^p$ where $g(x)$ has coefficients in $\mathfrak{K}$. We may now prove that in fact $f(x, \bar{t})$ is irreducible in $\mathfrak{K}$.

By hypothesis t is in T and hence $f(x, \bar{t})$ is irreducible in $\mathfrak{F}$. Let $f(x, \bar{t}) = f_0(x) \cdot f_1(x)$ where f_0 and f_1 have coefficients in $\mathfrak{K}$, $f_0(x)$ is irreducible in $\mathfrak{K}$, and neither is a constant polynomial in x. Then at least one coefficient of $f_0(x)$ is not in $\mathfrak{F}$ and, by the proof of Lemma 2, there exists an α in $\mathfrak{F}$ such that the constant term of $f_0(x + \alpha)$ is not in $\mathfrak{F}$. By the proof of Lemma 3 the polynomial $F_0(x + \alpha) = [f_0(x + \alpha)]^p$ is irreducible in $\mathfrak{F}$. Then $[f(x + \alpha, \bar{t})]^p = F_0(x + \alpha) \cdot [f_1(x + \alpha)]^p$ and necessarily

$$f(x + \alpha, \bar{t}) = F_0(x + \alpha) \equiv [f_0(x + \alpha)]^p\,, \qquad f(x, \bar{t}) \equiv [f_0(x)]^p\,,$$

contrary to the above proof. Thus we have Lemma 5.

4. A **Hilbert Irreducibility Theorem.** We now prove our Theorem 1. Consider a set of polynomials $f_i(x, t)$ of the form (2) and let the coefficients of the powers of x in $f_{\sigma+1}(x, t), \cdots, f_\mu(x, t)$ be all polynomials in t^p while each $f_i(x, t)$ has at least one coefficient $c_i(t)$ not a polynomial in t^p for $i = 1, \cdots, \sigma$. We may then write

$$c_i(t) = \sum_{j=0}^{p-1} \delta_{ij}(t^p)t^j = \sum_{j=0}^{p-1} \gamma_{ij}(t)\, z^j \qquad (i = 1, \cdots, \sigma)\,,$$

where the $\gamma_{ij}(t)$ have coefficients in $\mathfrak{F}$. Put $t = \lambda z + \rho$ and obtain

$$c_i(t) = \sum_{j=0}^{p-1} d_{ij}\,(\lambda, \rho)\, z^j\,,$$

where the d_{ij} have coefficients in $\mathfrak{F}$. At least one $d_{ij_i}(\lambda, \rho) \not\equiv 0$ in λ and ρ for $j_i > 0$. For when $c_i(t)$ has coefficients in $\mathfrak{F}$ then so have the $\delta_{ij}(t^p)$ and $d_{ij_i}(\lambda, 0) = \delta_{ij_i}(\lambda^p d)\lambda^j \not\equiv 0$ for at least one $j_i > 0$. When $c_i(t)$ does not have all its coefficients in $\mathfrak{F}$ then $d_{ij_i}(0, \rho) = \gamma_{ij_i}(\rho) \not\equiv 0$ for at least one $j_i > 0$. The field $\mathfrak{F}$ is an infinite field and there exist quantities λ_0, ρ_0 in $\mathfrak{F}$ for which the $d_{ij_i}(\lambda_0, \rho_0)$ are all not zero. We put $\tau = \lambda_0 z + \rho_0$ and have proved that the polynomials

$$g_i(x, t) \equiv f_i(x, t + \tau) \qquad (i = 1, \cdots, \mu), \tag{10}$$

have coefficients either not in $\mathfrak{F}(t)$ or coefficients which are polynomials in $(t + \tau)^p = t^p + \tau^p$ and hence are in $\mathfrak{F}(t^p)$. The polynomials $g_i(x, t)$ obviously have the form (2) and are irreducible in $\mathfrak{K}(t)$. By Lemmas 2, 3, 5 we may define a set of corresponding polynomials $F_i(x, t)$ with coefficients in $\mathfrak{F}$ and irreducible in $F(t)$. Moreover if T is the set of all quantities $\bar{t}$ of $\mathfrak{F}$ such that the $F_i(x, \bar{t})$ are simultaneously irreducible in $\mathfrak{F}$ then the $g_i(x, \bar{t})$ are simultaneously irreducible in $\mathfrak{K}$ for all but a finite number of $\bar{t}$ in T. But $\mathfrak{F}$ is an H.I. field, T is an infinite set, and $g_i(x, \bar{t}) \equiv f_i(x, \tau + \bar{t})$. Hence the $f_i(x, t)$ are simultaneously irreducible in $\mathfrak{K}$ for infinitely many quantities $\tau + \bar{t}$ of $\mathfrak{K}$. We have proved Theorem 1.

II. INVOLUTORIAL SIMPLE ALGEBRAS

1. **An involution of $\mathfrak{A}$.** Let $\mathfrak{A}$ be a simple algebra over an arbitrary field $\mathfrak{F}$ and let there be a correspondence

$$J: \qquad a \leftrightarrow a^J \qquad (a, a^J \text{ in } \mathfrak{A}),$$

of $\mathfrak{A}$ such that

$$(a + b)^J = a^J + b^J, \quad (ab)^J = b^J a^J, \quad (a^J)^J = a, \quad \lambda^J = \lambda, \tag{11}$$

for every a and b of $\mathfrak{A}$ and λ of $\mathfrak{F}$. *Then we shall call J an involution of $\mathfrak{A}$ and say that $\mathfrak{A}$ is J-involutorial.*

A quantity a of $\mathfrak{A}$ will be called J-symmetric if $a^J = a$ and J-skew if $a^J = -a$. If every quantity of algebra $\mathfrak{A}$ is J-symmetric then $ab = (ab)^J = b^J a^J = ba$ and $\mathfrak{A}$ *is a commutative algebra.* Then $\mathfrak{A}$ is an algebraic field of finite degree over $\mathfrak{F}$.

2. **The centrum of $\mathfrak{A}$.** Let $\mathfrak{K}$ be the centrum of $\mathfrak{A}$ and $\mathfrak{K}_0$ be the set of all J-symmetric quantities of $\mathfrak{K}$. Then we call $\mathfrak{A}$ *an algebra of the first or second kind according as $\mathfrak{K} = \mathfrak{K}_0$ or $\mathfrak{K} \neq \mathfrak{K}_0$.*

The field $\mathfrak{K}$ consists of all k's of $\mathfrak{A}$ such that $ka = ak$ for every a of $\mathfrak{A}$. Thus $ka^J = a^J k$ and $ak^J = k^J a$ for every a of $\mathfrak{A}$ and k of $\mathfrak{K}$. Hence $\mathfrak{K}$ is J-involutorial. We shall prove

THEOREM 2. *The field* $\mathfrak{K}$ *is either* $\mathfrak{K}_0$ *or a separable quadratic extension* $\mathfrak{K} = \mathfrak{K}_0(q)$ *of* $\mathfrak{K}_0$. *Moreover in the latter case we may take*[28]

$$q^J = -q, \qquad q^2 = \mu \text{ in } \mathfrak{K}_0, \tag{12}$$

when the characteristic of $\mathfrak{F}$ *is not two, and*

$$q^J = q + 1, \qquad q^2 = q + \mu, \qquad \mu \text{ in } \mathfrak{K}_0, \tag{13}$$

when $\mathfrak{F}$ *has characteristic two.*

For let the characteristic of $\mathfrak{F}$ be different from two and $\mathfrak{K} \neq \mathfrak{K}_0$ so that $q \equiv k_0 - k_0^J \neq 0$ for at least one k_0 of $\mathfrak{K}$. Put

$$\mu = q^2, \qquad 2k_1 = k + k^J, \qquad 2k_2 = (k - k^J)\mu^{-1} q, \tag{14}$$

for every k of $\mathfrak{K}$. Then $q^J = k_0^J - k_0 = -q$ is not in $\mathfrak{K}_0$ but $\mu = q^2 = (q^J)^2 = \mu^J$ is in $\mathfrak{K}_0$. Also

$$k = k_1 + k_2 q \tag{15}$$

where $k_1 = k_1^J$ and $k_2 = k_2^J$ are in $\mathfrak{K}_0$. Hence $\mathfrak{K} = \mathfrak{K}_0(q)$. We next let $\mathfrak{F}$ have characteristic two and see that every quantity k of $\mathfrak{K}$ is a root of

$$w^2 - (k + k^J)w + kk^J = 0$$

with coefficients in $\mathfrak{K}_0$. If $k + k^J = 0$ then $2 = 0, -1 = 1$ in $\mathfrak{F}$ gives $k = k^J$ is in $\mathfrak{K}_0$. Thus $\mathfrak{K} \neq \mathfrak{K}_0$ implies that at least one $k_0 \neq k_0^J$. Write

$$q = (k_0 + k_0^J)^{-1} k_0, \qquad \mu = (k_0 + k_0^J)^{-2} k_0 k_0^J,$$

so that μ is in $\mathfrak{K}_0$ and

$$q^2 = q + \mu. \tag{16}$$

The cyclic equation $q^2 - q - \mu = 0$ has roots $q, q + 1$ in $\mathfrak{K}$ and also $(q^J)^2 = q^J + \mu$. Then $q^J = q + 1$. Write

$$k_1 = k + (k + k^J)q, \qquad k_2 = k + k^J, \tag{17}$$

so that $k_2 = k_2^J$ is in $\mathfrak{K}_0$ and $k_1^J = k^J + (k + k^J)(q + 1) k^J + (k + k^J) + (k + k^J)q = k_1$ is in $\mathfrak{K}_0$. Then every k of $\mathfrak{K}$ has the property $k = k_1 + k_2 q$ where k_1 and k_2 are in $\mathfrak{K}_0$. Hence $\mathfrak{K} = \mathfrak{K}_0(q)$ is a separable quadratic extension of $\mathfrak{K}_0$ and we have Theorem 2.

If $\mathfrak{A}$ is an algebra of the second kind over its centrum $\mathfrak{K}_0(q)$ then we may write

$$a = \tfrac{1}{2}(a + a^J) + [\tfrac{1}{2}(a - a^J)\mu^{-1}q]q = a_1 + a_2 q,$$

[28] Similar results were obtained by C. Rosati (3) and A. A. Albert (1) for the case of the multiplication algebras of Riemann materials over a field $\mathfrak{F}$ of characteristic zero. Our treatment of the case where the characteristic of $\mathfrak{F}$ is two is new, however.

when $\mathfrak{F}$ has characteristic not two, and

$$a = [a + (a + a^J)q] + (a + a^J)q = a_1 + a_2 q,$$

when $\mathfrak{F}$ has characteristic two. In either case the above proof for $\mathfrak{K}$ shows that the quantities a_1 and a_2 are J-symmetric and if $\mathfrak{B}$ over $\mathfrak{K}_0$ is the linear set of all J-symmetric quantities of $\mathfrak{A}$ then $\mathfrak{A} = \mathfrak{B}_{\mathfrak{K}}$. We have proved

THEOREM 3. *Let $\mathfrak{A}$ be a J-involutorial simple algebra of the second kind of order m over its centrum $\mathfrak{K}$. Then $\mathfrak{A}$ has a basis*

$$u_1, \cdots, u_m \qquad (u_i^J = u_i),$$

over $\mathfrak{K}$.

3. **The involutions of $\mathfrak{A}$.** Let $\mathfrak{A}$ be a simple algebra with an involution J and let T be a new involution of $\mathfrak{A}$ such that $k^T = k^J$ for every k in the centrum of $\mathfrak{A}$. Then we call T *a J-centrum preserving involution of* $\mathfrak{A}$ and wish to determine all such involutions T.

The correspondence $a^J \leftrightarrow a^T$ satisfies the properties

$$(18) \qquad \begin{aligned} a^J + b^J = (a + b)^J \leftrightarrow (a + b)^T &= a^T + b^T, \qquad k^J = k^T \\ a^J b^J = (ba)^J \leftrightarrow (ba)^T &= a^T b^T \end{aligned}$$

for every a^J and b^J of $\mathfrak{A}$ and k of $\mathfrak{K}$. Hence the above correspondence of $\mathfrak{A}$ is an *automorphism* of the simple algebra $\mathfrak{A}$ *over its centrum.* It is well known that every such automorphism is an inner automorphism,[29] that is,

$$a^T = p^{-1} a^J p,$$

where p is a *regular* element of $\mathfrak{A}$. But

$$(a^T)^T = p^T (a^J)^T (p^{-1})^T = (p^{-1} p^J p)(p^{-1} a p)[p^{-1} (p^J)^{-1} p] = (p^{-1} p^J) a (p^{-1} p^J)^{-1} = a$$

so that $p^{-1} p^J$ is commutative with every quantity of $\mathfrak{A}$ and is in its centrum.

We write $p^{-1} p^J = \delta$, $p^J = p\delta$. Then $(p^J)^J = p = \delta^J p^J = \delta^J \delta p$ and $\delta^J \delta = 1$. If $\delta^J = \delta$ then $\delta^2 = 1$, $\delta = \pm 1$ and p is either J-symmetric or J-skew. If $\delta \neq \delta^J$ then $\mathfrak{K} \neq \mathfrak{K}_0$, $\mathfrak{K} = \mathfrak{K}_0(q)$ and $\delta = \delta_1 + \delta_2 q$, $\delta_1^2 - \delta_2^2 \mu = \delta\delta^J = 1$. But then it is known that $\delta = \gamma(\gamma^J)^{-1}$ with γ in $\mathfrak{K}$. Hence $p_0 = \gamma p$ has the property $p_0^J = p^J \gamma^J = p\delta\gamma^J = p\gamma = p_0$ and is J-symmetric. Obviously $a^T = p^{-1} a^J p = p_0^{-1} a^J p_0$.

Conversely let us define the correspondence $a \leftrightarrow a^T = p^{-1} a^J p$ where p is either J-symmetric or J-skew. Then

$$\begin{aligned} (a + b)^T &= p^{-1}(a + b)^J p = p^{-1}(a^J + b^J)p = a^T + b^T, \\ (ab)^T &= p^{-1}(ab)^J p = p^{-1}(b^J a^J)p = (p^{-1} b^J p)(p^{-1} a^J p) = b^T a^T, \\ k^T &= p^{-1} k^J p = k^J, \qquad \lambda^T = p^{-1} \lambda^J p = \lambda, \\ (a^T)^T &= (p^{-1} p^J) a (p^{-1} p^J)^{-1} = (\pm 1) a (\pm 1)^{-1} = a \end{aligned}$$

for every a and b of $\mathfrak{A}$, k of $\mathfrak{K}$ and λ of $\mathfrak{F}$. We have proved

[29] Cf. Brauer (1), Theorem 11.

THEOREM 4. *Let $\mathfrak{A}$ be a J-involutorial simple algebra and $a \leftrightarrow a^T$ be a self-correspondence of $\mathfrak{A}$. Then T is a J-centrum preserving involution of $\mathfrak{A}$ if and only if there exists a regular J-symmetric or J-skew quantity p of $\mathfrak{A}$ such that*

$$a^T = p^{-1}a^J p. \tag{19}$$

We also have the

COROLLARY. *Let Z be a maximal sub-field of $\mathfrak{A}$ and $z^T = z^J$ for every z of Z. Then* (4) *holds with p in Z.*

For the only quantities of $\mathfrak{A}$ commutative with every quantity of Z are the quantities of Z. But $z^T = p^{-1}z^Jp = z^J$ implies that $pz^J = z^Jp$ and hence $zp = pz$, since $(z^J)^J = z$, $p^J = \pm p$. Thus p is in Z.

4. **The Wedderburn decomposition of $\mathfrak{A}$.** We may write[30] $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$ where $\mathfrak{M}$ is a total matric algebra and $\mathfrak{D}$ is a division algebra whose centrum is that of $\mathfrak{A}$. Then $\mathfrak{M}$ has an ordinary matric basis[31] e_{ij} and a multiplication table

$$e_{ij}e_{tk} = \delta_{jt}e_{ik} \qquad (i, j, t, k = 1, \cdots, m)$$

where $\delta_{jj} = 1$, $\delta_{jt} = 0$ for $j \neq t$.

Write $f_{ij} = e^J_{ji}$. Then $f_{ij}f_{tk} = e^J_{ji}e^J_{kt} = (e_{kt}e_{ji})^J = (\delta_{tj}e_{ki})^J = \delta_{tj}f_{ik}$ so that the quantities of f_{ij} form a basis of a total matric algebra $\mathfrak{M}_0$ equivalent to $\mathfrak{M}$. Moreover $\mathfrak{A} = \mathfrak{M}_0 \times \mathfrak{D}_0$ and it is well known[29] that the resulting automorphism of $\mathfrak{A}$ is *an inner automorphism,* that is

$$f_{ij} = pe_{ij}p^{-1} = e^J_{ji},$$

where p is a regular element of $\mathfrak{A}$.

We compute $(e^J_{ji})^J = e_{ji} \doteq (p^J)^{-1}e^J_{ij}p^J = (p^{-1}p^J)^{-1}e_{ji}(p^{-1}p^J)$ and have shown that $p^{-1}p^J$ is in the algebra of all quantities of $\mathfrak{A}$ commutative with all the e_{ij}. This algebra is $\mathfrak{D}$ so that $p^J = p\delta$ with δ in $\mathfrak{D}$.

If $\delta \neq -1$ the quantity $p_0 = p + p^J = p(1 + \delta)$ is obviously both regular and J-symmetric. Moreover $f_{ij} = p_0e_{ij}p_0^{-1}$ since $1 + \delta$ is commutative with all the e_{ij}. Hence in this case we may take $p = p^J$ without loss of generality. If $\delta = -1$ then $p^J = -p$ and p is J-skew. In either case the correspondence $a \leftrightarrow a^T = p^{-1}a^Jp$ is a centrum preserving involution of $\mathfrak{A}$ with the property

$$e^T_{ij} = p^{-1}e^J_{ij}p = e_{ji}.$$

Algebra $\mathfrak{D}$ is the algebra of all quantities of $\mathfrak{A}$ commutative with all the e_{ij}. If d is in $\mathfrak{D}$ then $de_{ji} = e_{ji}d$, $de^T_{ij} = e^T_{ij}d$, $e_{ij}d^T = d^Te_{ij}$ and d^T is in $\mathfrak{D}$. We have proved the important

THEOREM 5. *Let $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$ be a J-involutorial simple algebra where $\mathfrak{D}$ is a division algebra and $\mathfrak{M}$ is a total matric algebra with ordinary matric basis e_{ij}.*

---

[30] Cf. Wedderburn (4), p. 158.

[31] For this terminology see Albert (1).

Then there exists a J-centrum preserving involution T of $\mathfrak{A}$ such that T is an involution of $\mathfrak{D}$ and

$$e_{ij}^{T} = e_{ji}. \tag{20}$$

5. **Symmetric sub-fields of $\mathfrak{A}$.** In this section we shall prove

THEOREM 6. *Let x be a quantity of $\mathfrak{A}$ and let the minimum equation of $\mathfrak{A}$ be irreducible in $\mathfrak{K}$ and have coefficients in $\mathfrak{K}_0$. Then there exists a J-centrum preserving involution T of $\mathfrak{A}$ such that*

$$x^T = x.$$

For the algebra X of all quantities of $\mathfrak{A}$ commutative with x is a normal simple algebra over $\mathfrak{K}(x)$. We may write $X = \mathfrak{M}_0 \times \mathfrak{B}$ where $\mathfrak{M}_0$ is a total matric algebra and $\mathfrak{B}$ is a normal division algebra over $\mathfrak{K}(x)$.

By Wedderburn's theorem we have $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D} = \mathfrak{M}_0 \times \mathfrak{A}_1 = \mathfrak{M}_0 \times \mathfrak{M}_1 \times \mathfrak{D}$. By Theorem 2 the algebra $\mathfrak{D}$ may be taken to be J-involutorial. Then J may be so chosen that $\mathfrak{A}_1 = \mathfrak{M}_1 \times \mathfrak{D}$ is J-involutorial and the sub-algebra of all quantities of $\mathfrak{A}_1$ commutative with x is a division algebra $\mathfrak{B}$.

The minimum equation $\phi(\xi) = 0$ of x has coefficients in $\mathfrak{K}_0$ and $\phi(x) = 0$ implies that $\phi(x^J) = 0$. But then x^J is a transform of x by a regular quantity p of $\mathfrak{A}_1$, $x^J = pxp^{-1}$. Consequently $x = (p^J)^{-1}x^Jp^J = (p^{-1}p^J)^{-1}xp^{-1}p^J$.

The quantity $p^{-1}p^J = y$ is in $\mathfrak{B}$, a division algebra. If $y \neq -1$ then $p_0 = p + p^J = p(1 + y)$ is regular and $p_0p_0^{-1} = p(1 + y)(1 + y)^{-1}p^{-1} = pp^{-1} = x^J$. If $y = -1$ then $p^J = -p$ is J-skew.

We have proved that $x^J = pxp^{-1}$ where p is either J-symmetric or J-skew. The self-correspondence $a \leftrightarrow a^T = p^{-1}a^Tp$ is a J-centrum preserving involution of $\mathfrak{A}_1$ by Theorem 2 and moreover $x^T = p^{-1}x^Jp = x$.

It is obvious that then there exists a J-centrum preserving involution of $\mathfrak{A} = \mathfrak{M}_0 \times \mathfrak{A}_1$ such that $x^T = x$. This proves Theorem 6.

6. **Involutions of $D_1 \times D_2$.** If $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are J-involutorial, the algebra $\mathfrak{A}_1 \times \mathfrak{A}_2$ is also J-involutorial. We may now prove a partial converse of this result.

We let $\mathfrak{D} = \mathfrak{D}_1 \times \mathfrak{D}_2$ be a J-involutorial division algebra and let $\mathfrak{D}_1$ and $\mathfrak{D}_2$ be direct factors of $\mathfrak{D}$ of relatively prime degrees. We may then prove

THEOREM 7. *There exists a J-centrum preserving involution T of $\mathfrak{D}$ such that both $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are T-involutorial.*

For let ρ_i be the exponent of $\mathfrak{D}_i$ and hence ρ_1 and ρ_2 relatively prime. Then the congruences

$$\xi = 1(\text{mod } \rho_1), \qquad \xi = 0(\text{mod } \rho_2)$$

have a solution ξ in common and $\mathfrak{D}^\xi = \mathfrak{D}_1^\xi \times \mathfrak{D}_2^\xi = \mathfrak{D}_1 \times \mathfrak{M}$ where $\mathfrak{M}$ is a total matric algebra. By Theorem 2 algebra $\mathfrak{D}_1$ is T-involutorial. We have a similar result for $\mathfrak{D}_2$ and have proved Theorem 7.

7. **Elementary properties of crossed products.**[32] Let $\mathfrak{D}$ be a division algebra of degree n over its centrum $\mathfrak{K}$ and Z be a field containing $\mathfrak{K}$. Then the algebra $\mathfrak{D} \times Z = \mathfrak{D}_Z$ is a normal simple algebra over Z and we say that Z splits $\mathfrak{D}$ if $\mathfrak{D}_Z$ is a total matric algebra.

If $\mathfrak{M}$ is a total matric algebra then $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$ is similar to $\mathfrak{D}$ and we write $\mathfrak{A} \sim \mathfrak{D}$. It is well known that there exist galois splitting fields Z of degree m over $\mathfrak{K}$ of $\mathfrak{D}$, that necessarily $m = ne$, and that Z is isomorphic to a maximal sub-field of $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$ where $\mathfrak{M}$ has degree e.

We assume that S ranges over all the m automorphisms $y \leftrightarrow y^S$ of Y. Then $\mathfrak{A}$ has a Y-basis u_S and every quantity of $\mathfrak{A}$ has the form $\Sigma\, u_S y_S$ with y_S in Y. The multiplication table of $\mathfrak{A}$ is given by

$$y u_S = u_S y^S, \qquad u_S u_T = u_{ST} a_{S,T}$$

with $a_{S,T} \neq 0$ in Y. The set $a = (a_{S,T})$ is called a factor set of $\mathfrak{A}$ and is replaced by an associated factor set $b = (b_{S,T})$,

$$b_{S,T} = a_{S,T} \frac{c_T c_S^T}{c_{S,T}}, \qquad (c_S \text{ in } Y), \tag{21}$$

when we replace the u_S by a new Y-basis $u_S c_S$. We write $\mathfrak{A} = (Y, a)$ and call $\mathfrak{A}$ the crossed product of Y and a.

A crossed product is a total matric algebra if and only if its factor set is associated with $1 = (1) = (b_{ST})$ with $b_{ST} = 1$. We also have the important direct product formula,

$$(Y, a) \times (Y, b) = (Y, 1) \times (Y, ab), \tag{22}$$

where $ab = (a_{ST} b_{ST})$.

We shall consider crossed products defined by galois fields (Z, Ω) over Ω where Z is a galois extension of degree n of an arbitrary field $\mathfrak{F}$ and Ω contains $\mathfrak{F}$. Suppose that Λ is an algebraically closed extension of Ω. By passing to a field isomorphic to Z we may assume that Λ contains Z. Write $Z = \mathfrak{F}(x_1)$ where

$$\phi(\xi) \equiv (\xi - x_1)\,(\xi - x_2)\,\cdots\,(\xi - x_n)$$

has coefficients in $\mathfrak{F}$ and is irreducible in $\mathfrak{F}$. Then $x_2, \cdots, x_n$ are in Z and the automorphisms of Z are generated by the correspondences $x_1 \leftrightarrow x_i$.

The composite (Z, Ω) of Z and Ω is the sub-field of Λ consisting of all rational functions of x_1 with coefficients in Ω. If $\psi(\xi) = 0$ is the factor of $\phi(\xi) = 0$ which is irreducible in Ω and has x_1 as a root then

$$\psi(\xi) \equiv (\xi - x_1) \cdots (\xi - x_\nu),$$

and (Z, Ω) is a galois field of degree ν over Ω. The coefficients of $\psi(\xi)$ lie in the sub-field of Y of Z generated by the elementary symmetric functions of

[32] For proofs of these properties see Hasse (2).

$x_1, \cdots, x_\nu$. Since Y is contained in Ω the equation $\psi(\xi)$ is irreducible in Y and Z has degree ν over Y. Thus

$$n = n_0 \nu,$$

where Y has degree n_0 over $\mathfrak{F}$. We have

THEOREM 8. *Let Z be a galois field of degree n over $\mathfrak{F}$, Ω be a field containing $\mathfrak{F}$, n_0 be the maximum degree over $\mathfrak{F}$ of all sub-fields of Z which are equivalent to sub-fields of Ω. Then $n = n_0\nu$ and ν is the degree of the composite (Z, Ω) over Ω.*

As an immediate consequence we obtain

THEOREM 9. *The direct product $Z \times \Omega$ of a normal field Z over $\mathfrak{F}$ and $\Omega > \mathfrak{F}$ is the composite (Z, Ω) if and only if Z has no sub-field distinct from $\mathfrak{F}$ and equivalent to a sub-field of Ω.*

We consider in particular the case where Z_0 is galois over $\mathfrak{K}_0$, $\Omega = \mathfrak{K} = \mathfrak{K}_0(q)$ is a separable quadratic extension of $\mathfrak{K}_0$. We then have the simple

LEMMA. *The composite $Z = (\mathfrak{K}_0, \mathfrak{K}) = Z_0 \times \mathfrak{K}$ if and only if Z_0 has no quadratic sub-field equivalent to $\mathfrak{K}_0$.*

8. **On J-involutorial crossed products.** Let $\mathfrak{D}$ be a division algebra over its centrum $\mathfrak{K}$ and let $\mathfrak{K} = \mathfrak{K}_0$ or $\mathfrak{K} = \mathfrak{K}_0(q)$ where $\mathfrak{K}_0(q)$ is a separable quadratic extension of $\mathfrak{K}_0$. The field $\mathfrak{K}$ is J-involutorial over $\mathfrak{K}_0$ and either $q^J = -q$ or $q^J = q + 1$. We *assume* that there exists a galois field Z_0 of degree m over $\mathfrak{K}_0$ such that $Z = Z_0 \times \mathfrak{K}$ is a splitting field of $\mathfrak{D}$. Then $\mathfrak{D}$ is similar to a crossed product (Y, a) where $Y = (Y_0, \mathfrak{K})$, Y_0 is equivalent to Z_0, Y is galois over $\mathfrak{K}$. We seek necessary and sufficient conditions that $\mathfrak{D}$ be J-involutorial over $\mathfrak{K}_0$ with the involution J of $\mathfrak{K}$ preserved.

Consider the algebra $\mathfrak{B} = (Y_0, a\bar{a})$ over $\mathfrak{K}_0$ where, if $a_{S,T} = a_{S,T1} + a_{S,T2}q$ with $a_{S,T1}$ and $a_{S,T2}$ in Y_0 then $\bar{a}_{S,T} = a_{S,T1} + a_{S,T2}q^J$. It is evident that the algebra $\bar{\mathfrak{A}} = (Y, \bar{a})$ is a crossed product and is a simple algebra over $\mathfrak{K}_0$ equivalent to $\mathfrak{A}$ over $\mathfrak{K}_0$ by a correspondence in which $q \leftrightarrow q^J$. Hence $\mathfrak{K} \times \mathfrak{B} \sim \mathfrak{A} \times \bar{\mathfrak{A}}$. We may now easily prove

THEOREM 10. *The algebra $\mathfrak{A}$ is J-involutorial if and only if $\mathfrak{B}$ is a total matric algebra.*

For let $\mathfrak{A}$ be J-involutorial so that, by Theorem 3, we may let $y^J = y$, $(y^S)^J = y^S$ for every y of Y_0. Then $u_S^J y = y^S u_S^J$, $u_S u_S^J y = u_S y^S u_S^J = y u_S u_S^J$. The symmetric quantity $p_S = u_S u_S^J$ is commutative with every y of Y_0 and must then be in Y_0. Hence $(u_S^J)^{-1} = b_S^{-1} u_S = u_S c_S$ where $c_S \neq 0$ is in Y_0.

Since $\mathfrak{A}$ is J-involutorial we have $u_T^J u_S^J = \bar{a}_{S,T} u_{ST}^J$ and hence $(u_S^J)^{-1}(u_T^J)^{-1} = (u_{ST}^J)^{-1}(\bar{a}_{S,T})^{-1}$. But $(u_S^J)^{-1} = u_S c_S$ so that the factor set $(\bar{a}_{S,T})^{-1}$ has the property

$$\bar{a}_{S,T}^{-1} = a_{S,T} \frac{c_T c_S^T}{c_{ST}}. \tag{23}$$

But then the factor set $(a_{S,T}\bar{a}_{S,T})$ of $\mathfrak{B}$ over $\mathfrak{K}_0$ is associated with the factor set consisting of unity alone and $\mathfrak{B}$ is a total matric algebra.

Conversely let $\mathfrak{B}$ be a total matric algebra so that we have (10) for c_S in Y_0.

We then define a correspondence J of $\mathfrak{A}$ by

$$[\sum u_S(y_{S1} + y_{S2}q)]^J = \sum(y_{S1} + y_{S2}q^J)(u_Sc_S)^{-1}.$$

Then $\mathfrak{A}$ is J-involutorial if and only if

$$(24) \qquad (u_S^J)^J = u_S, \qquad u_S^J y = y^S u_S^J, \qquad u_T^J u_S^J = a_{S\,T}^J u_{S\,T}^J,$$

for every y of Y_0. But $(u_S^J)^J = [(u_Sc_S)^{-1}]^J = [c_S^{-1}u_S^{-1}]^J = (u_S^J)^{-1}c_S^{-1} = u_Sc_Sc_S^{-1} = u_S$ as desired. Since $u_Sy^S = yu_S$ we have $u_Sc_Sy^S = yu_Sc_S$ so that $u_S^Jy = y^Su_S^J$. Finally $u_Su_T = u_{ST}a_{S,T}$, $(u_Sc_S)(u_Tc_T) = (u_{ST}c_{ST})b_{S,T}$ with

$$b_{S,T} = a_{S,T}\frac{c_Sc_T}{c_{ST}} = (a_{S,T}^J)^{-1},$$

so that (23) is obtained by taking reciprocals. This proves Theorem 10.

If J_0 is any new involution of $\mathfrak{A}$ such that $y_0^{J_0} = y_0$ for every y_0 of Y_0 then, by Corollary I, we have

$$(25) \qquad a^{J_0} = p^{-1}a^Jp$$

where $p^J = \pm p$ is in Y. If p is not in Y_0 then pq is in Y_0 and has the above property (13). Hence we may take p in Y_0. Then

$$u_S^{J_0} = p^{-1}u_S^Jp = (u_Sd_S)^{-1}$$

where $[p^{-1}(u_Sc_S)^{-1}p]^{-1} = p^{-1}u_Sc_Sp = u_S(p^S)^{-1}c_Sp$ and

$$(26) \qquad d_S = (p^S)^{-1}pc_S. \qquad (p \text{ in } Y_0).$$

Moreover d_S satisfies the equation (23) in c_S. Conversely every solution c_S of (23) defines an involution J_0 of $\mathfrak{A}$ by Theorem 10 and hence satisfies (26). We have

THEOREM 11. *If c_S is any solution of* (23) *then all solutions d_S are given by* (26) *and all involutions J_0 such that the quantities of Y_0 are J_0-symmetric are given by* (25).

We shall call the algebras $\mathfrak{A}$ defined above and satisfying the properties of Theorem 10 *algebras of type* A. We now consider the special case where $\mathfrak{D}$ is a J-involutorial division algebra of the first kind.

When $\mathfrak{D}$ is of the first kind it is self reciprocal and it is well known that $\mathfrak{D}^2$ is a total matric algebra. Conversely if $\mathfrak{D}^2$ is a total matric algebra then it is self-reciprocal and the self-correspondence thereby induced is a reciprocal automorphism. This automorphism is obviously not necessarily an involution. We have however proved that if $\mathfrak{D}$ is a division algebra of exponent two and $\mathfrak{A}$ is the crossed product similar to $\mathfrak{D}$ so that $\mathfrak{A}^2 \sim \mathfrak{B}$ is a total matric algebra then $\mathfrak{A}$ is J-involutorial. By Theorem 5 so is $\mathfrak{D}$ and we have proved

THEOREM 12. *A normal division algebra is J-involutorial of the first kind over its centrum $\mathfrak{K}$ if and only if it is self-reciprocal, that is has exponent* 1 *or* 2.

9. **Cyclic Algebras.** We may consider in particular *cyclic algebras of type* A.

In this case Z_0 is cyclic over $\mathfrak{K}_0$ and hence Y_0 is cyclic over $\mathfrak{K}_0$ with generating automorphism S. There exists a quantity u in $\mathfrak{A}$ such that

$$(y_1 + y_2q)u = u(y_1^S + y_2^Sq),$$

for every y_1 and y_2 of Y_0 and $1, u, \cdots, u^{n-1}$ form a Y-basis of $\mathfrak{A}$. The quantity $u^n = \gamma$ is in $\mathfrak{K}$ and has a norm $\gamma\gamma^J$ with respect to $\mathfrak{K}_0$. By Theorem 10 we have

THEOREM 13. *The cyclic algebra $\mathfrak{A}$ is J-involutorial if and only if there exists a quantity d of Y_0 such that*

$$N_{\mathfrak{K}/\mathfrak{K}_0}(\gamma) = N_{Y_0/\mathfrak{K}_0}(d).$$

We shall also define a further type of algebra over a special field $\mathfrak{K}_0$. Let π be the field of residue classes modulo a prime p, and $\mathfrak{K}_0$ be an infinite field with π as prime sub-field. Suppose that $\pi(z)$ is an algebraic extension of degree μ over π so that[33]

$$\pi(z) = GF(p^\mu).$$

Every sub-field of $\pi(z)$ is a finite field $GF(p^\tau)$ and if the largest finite sub-field of K_0 is equivalent to $GF(p^\sigma)$, then

$$\mu = \sigma\nu,$$

and Theorem 8 states that the composite $\mathfrak{K}_0(z)$ has degree ν over $\mathfrak{K}_0$. The field $\mathfrak{K} = \mathfrak{K}_0(q)$ is a quadratic extension of $\mathfrak{K}_0$ and the composite $\mathfrak{K}_0(q, z)$ has degree ν over $\mathfrak{K}$ if and only if no quadratic sub-field of $\mathfrak{K}_0(z)$ is equivalent to $\mathfrak{K}_0(q)$. But $\mathfrak{K}_0(q, z) = \mathfrak{K}(z)$ has degree ν over $\mathfrak{K}$ if and only if $\mathfrak{K}$ does not contain a sub-field equivalent to a finite field of degree greater than σ. Hence we have

THEOREM 14. *Let $\pi(z) = GF(p^\mu)$ and $\mathfrak{K} = \mathfrak{K}_0(q)$. Then the degree of $\mathfrak{K}(z)$ over $\mathfrak{K}$ is the degree of $\mathfrak{K}_0(z)$ over $\mathfrak{K}_0$ if and only if the largest finite sub-field of $\mathfrak{K}$ coincides with that of $\mathfrak{K}_0$.*

We assume that the largest finite sub-field of $\mathfrak{K}_0$ is $G_\sigma = GF(p^\sigma)$ while $\mathfrak{K}$ contains $G_{2\sigma} = GF(p^{2\sigma})$. Then we may take $G_{2\sigma} = G_\sigma(q)$ since it is evident that if $G_{2\sigma} = G_\sigma(q_0)$ then $\mathfrak{K} = \mathfrak{K}_0(q_0)$. Hence $G_{2\sigma} = \pi(q)$ where q is a primitive $\rho_{2\sigma}^{th}$ root of unity and

$$\rho_{2\sigma} = p^{2\sigma} - 1.$$

Moreover

$$\mu = 2\sigma n,$$

where $Z = \mathfrak{K}(z)$ is cyclic of degree n over $\mathfrak{K}$ and with generating automorphism

$$S: \qquad z \leftrightarrow z^\beta \qquad (\beta = p^{2\sigma}).$$

We now define a cyclic algebra $\mathfrak{A}$ with $1, u, \cdots, u^{n-1}$ as Z-basis and

$$zu = uz^\beta, \qquad u^n = \gamma \text{ in } \mathfrak{K}. \tag{27}$$

---

[33] Cf. Van der Waerden, vol. 1, p. 109.

Assume also that $\mathfrak{A}$ is not a total matric algebra and hence $n > 1$. We call $\mathfrak{A}$ *an algebra of type* B.

No power of γ is in π since otherwise the algebra $\mathfrak{B}$ with the same basal units as $\mathfrak{A}$ but over $\pi(q, \gamma)$ is a normal simple algebra over a finite field and hence is a total matric algebra.[34] Then $\mathfrak{A} = \mathfrak{B}_{\mathfrak{R}}$ is a total matric algebra contrary to hypothesis. In particular $1 + \gamma(-\gamma^2)^{n-1} \neq 0$ so that there exists an α_0 in $\mathfrak{R}$ such that

$$\alpha_0 [1 + \gamma(-\gamma^2)^{n-1}] = \gamma^{-1}(-\gamma^2)^{n-1}. \tag{28}$$

Then $\alpha_0 = (-\gamma^2)^{n-1}(\gamma^{-1} - \gamma\alpha_0)$. Define $\alpha_2, \cdots, \alpha_{n-1}$ in $\mathfrak{R}$ by

$$\alpha_{i-1} = -\gamma^2\alpha_i \qquad (i = 1, \cdots, n-1), \tag{29}$$

and obtain $\alpha_0 = (-\gamma^2)^{n-1}\alpha_{n-1}$, $\alpha_{n-1} = \gamma^{-1} - \gamma\alpha_0$. By a simple computation we have

$$(\gamma^2 + u)(\alpha_0 + \alpha_1 u + \cdots + \alpha_{n-1}u^{n-1}) = 1\,.$$

Hence $\gamma^2 + u$ is a regular quantity of algebra $\mathfrak{A}$.

The field $\mathfrak{R}_0(z)$ is cyclic of degree $2n$ over $\mathfrak{R}_0$ with generating automorphism

$$T: \qquad z \leftrightarrow z^T = z^S \qquad (\delta = p^\sigma),$$

and $T^2 = S$. Hence T replaces q by q^J, and if $\mathfrak{A}$ is J-involutorial over $\mathfrak{R}_0$ then z^δ is a root of the minimum equation of z^J with respect to $\mathfrak{R}$. By a well known theorem

$$z^J = a^{-1}z^\delta a$$

where a is a regular quantity of $\mathfrak{A}$. Moreover

$$z = a^J(z^\delta)^J(a^J)^{-1} = (a^Ja^{-1})z^{\delta^2}(a^Ja^{-1})^{-1}$$

so that

$$z(a^Ja^{-1}) = (a^Ja^{-1})z^S, \qquad u_0 = a^Ja^{-1}\,.$$

But then $u_0 = ud$ where d is in $\mathfrak{R}(z)$ and

$$u_0^n = \gamma N_{Z/\mathfrak{R}}(d) = \gamma_0\,. \tag{30}$$

Without loss of generality we take $u = u_0$ and have

$$a^J = ua\,, \qquad a = a^Ju^J = uau^J\,,$$

so that

$$u^J = a^{-1}u^{-1}a\,, \qquad (u^J)^n = \gamma^J = \gamma^{-1}\,.$$

We may now prove

THEOREM 15. *Algebra $\mathfrak{A}$ of type* B *is J-involutorial of the second kind if and only if there exists a γ_0 of* (30) *satisfying*

$$N_{\mathfrak{R}/\mathfrak{R}_0}(\gamma_0) = \gamma_0\gamma_0^J = 1\,. \tag{31}$$

[34] A theorem of J. H. M. Wedderburn, cf. Van der Waerden II, p. 211.

For we have proved the above condition necessary. Suppose now that $\gamma_0\gamma_0^J = 1$ so that we may take $\gamma\gamma^J = 1$ without loss of generality. We of course mean to imply that γ goes to γ^J when $q \leftrightarrow q^J = q^T$ under the automorphism T of $\mathfrak{K}_0(z)$. The quantity $\gamma^2 + a$ is a regular quantity of $\mathfrak{A}$ and hence so is

$$a = a^{-1}\gamma^{-1}(\gamma^2 + u) = \gamma^{-1} + \gamma u^{-1} = \gamma^J + u^{n-1}.$$

We now define a $(1 - 1)$ correspondence of $\mathfrak{A}$ by

$$z^J = a^{-1}z^\delta a, \qquad u^J = a^{-1}u^{-1}a = u^{-1}$$

since a is a polynomial in u. Then

$$(u^J)^n = \gamma^J = \gamma^1, \qquad u^Jz^J = (z^J)^\beta u^J,$$

since $u^{-1}a^{-1}z^\delta a = a^{-1}z^{\beta\delta}u^{-1}a = (z^J)^\beta u^J$ by our definitions. The minimum equation of z^J and z^δ is obtained from that of z by replacing q by q^J and hence J is a reciprocal automorphism of $\mathfrak{A}$. Finally $(u^J)^J = (u^{-1})^{-1} = u$ and we have proved that $(z^J)^J = z$ if $a^J a^{-1} = u$. But $ua = \gamma^J u + \gamma = a^J$ since $a^J = \gamma + u^{1-n} = \gamma + u\gamma^{-1} = \gamma + u\gamma^J$. We have proved Theorem 14.

10. **Algebras over a reduced field.** We have defined two types of J-involutorial simple algebras of the second kind and may now prove that these types give the structure of all J-involutorial simple algebras of the second kind. Let then $\mathfrak{A}$ be a J-involutorial simple algebra with centrum $\mathfrak{K} = \mathfrak{K}_0(q)$ over $\mathfrak{F}$ and let π be the prime sub-field of $\mathfrak{K}_0$. Then π is equivalent to the field of all rational numbers or all residue class modulo a prime p according as $\mathfrak{F}$ has characteristic zero or p. We shall call $\mathfrak{F}$ *a reduced field if it may be obtained from* π *by a finite number of adjunctions* (*algebraic or transcendental*).

If $u_1, \cdots, u_r$ are a basis of $\mathfrak{A}$ over $\mathfrak{F}$ then

$$u_iu_j = \sum_{k=1}^{r} \gamma_{ijk}u_k, \qquad u_i^J = \sum_{k=1}^{r} \delta_{ik}u_k$$

with γ_{ijk} and δ_{ik} in $\mathfrak{F}$. The field $\mathfrak{F}_0 = \pi(\delta_{11}, \cdots, \delta_{rr}, \gamma_{111}, \cdots, \gamma_{rrr})$ is a reduced field. Let $\mathfrak{B}$ be the algebra with basis $u_1, \cdots, u_r$ over $\mathfrak{F}_0$. Obviously $\mathfrak{A} = \mathfrak{B}_{\mathfrak{F}}$ and $\mathfrak{B}$ is a J-involutorial simple algebra over $\mathfrak{F}_0$. Conversely if $\mathfrak{B}$ is a J-involutorial simple algebra over $\mathfrak{F}_0$ and $\mathfrak{F}$ is an extension of $\mathfrak{F}_0$ such that $\mathfrak{A} = \mathfrak{B}_{\mathfrak{F}}$ is simple over $\mathfrak{F}$ then $\mathfrak{A}$ is a J-involutorial simple algebra over $\mathfrak{F}$. Moreover the involution of the centrum of $\mathfrak{A}$ is uniquely determined by that of $\mathfrak{B}$. We have

THEOREM 16. *A simple algebra $\mathfrak{A}$ over $\mathfrak{F}$ is J-involutorial of the second kind if and only if $\mathfrak{A} = \mathfrak{B}_{\mathfrak{F}}$ where $\mathfrak{B}$ is J-involutorial of the second kind over a reduced field $\mathfrak{F}_0$.*

We have only to consider the case where $\mathfrak{F}$ is a reduced field. If $\mathfrak{F}$ is a finite field then $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$ where $\mathfrak{M}$ is a total matric algebra and $\mathfrak{D}$ is a finite field. Then $\mathfrak{K} = \mathfrak{D}$ and the structure of $\mathfrak{A}$ is completely determined by Theorem 1. Assume therefore that $\mathfrak{F}$ is an infinite field. We prove

THEOREM 17. *A reduced field $\mathfrak{F}$ is an H.I. field if $\mathfrak{F}$ is not an algebraic extension of finite degree of $\Omega = \pi(\xi)$ where ξ is an indeterminate and π is finite.*

For if π is the field of rational numbers then $\mathfrak{F}$ is an H.I. field by Theorem F1 and F2. When π has characteristic p and $\mathfrak{F}$ is not finite there exists a quantity ξ in $\mathfrak{F}$ which is transcendental with respect to π. Then $\mathfrak{F}$ is not algebraic over $\Omega = \pi(\xi)$ and hence must contain a quantity η which is transcendental with respect to Ω. By Theorem F2 the field $\Omega(\eta)$ is an H.I. field. The field $\mathfrak{F}$ is obtained from $\Omega(\eta)$ by a finite number of adjunctions and $\mathfrak{F}$ is an H.I. field by Theorem 1 and Theorem F2. We may assume my

SYMMETRIC GROUP THEOREM.[35] *Let $\mathfrak{D}$ be a normal division algebra of order $m = n^2$ and basis $u_1, \cdots, u_m$ over its centrum $\mathfrak{K}$ which is a separable algebraic extension of an H.I. field $\mathfrak{K}_0$. Then there exist infinitely many quantities $\xi_1, \cdots, \xi_m$ of $\mathfrak{K}_0$ such that the minimum equation of $x = \sum_i \xi_i u_i$ has degree n and the symmetric group with respect to $\mathfrak{K}$.*

We use Theorem 3 to obtain a basis of J-symmetric quantities for $\mathfrak{D}$ over $\mathfrak{K}$ where $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$. By the above theorem there exists a J-symmetric quantity x in $\mathfrak{D}$ whose minimum equation $\phi(\xi) = 0$ then has coefficients in $\mathfrak{K}_0$, degree n, and the symmetric group with respect to $\mathfrak{K}$. Let η_1 be a scalar root of $\phi(\xi) = 0$ and $\eta_2, \cdots, \eta_n$ its scalar conjugates. Then the field $Z = \mathfrak{K}(\eta_1, \cdots, \eta_n)$ is well known to be a normal splitting field for $\mathfrak{D}$ and hence $\mathfrak{A}$. Let $Z_0 = \mathfrak{K}_0(\eta_1, \cdots, \eta_n)$ so that Z_0 is normal over $\mathfrak{K}_0$ and its automorphism group is isomorphic to the symmetric group on n letters. If the composite Z of Z_0 and K has its degree over $\mathfrak{K}$ less than the degree of Z_0 over $\mathfrak{K}_0$ then the automorphism group H of Z over $\mathfrak{K}$ is a proper sub-group of the group G of Z_0 over $\mathfrak{K}_0$. But H is evidently the galois group of $\phi(\xi) = 0$ and must be isomorphic to the symmetric group on n letters. Hence $H = G$, the degree of Z over $\mathfrak{K}$ is $n!$, the degree of Z_0 over $\mathfrak{K}_0$, and $Z = Z_0 \times \mathfrak{K}$. We have proved

THEOREM 18. *Let $\mathfrak{F}$ be an H.I. field and $\mathfrak{A}$ be a J-involutorial algebra of the second kind over $\mathfrak{F}$. Then $\mathfrak{A}$ is similar to an algebra of type* A.

The only remaining case is that where $\mathfrak{F}$ is algebraic of finite degree over $\Omega = \pi(\xi)$, π of characteristic p. It is known that there exists a finite field $\pi(z)$ such that $\mathfrak{K}(z)$ splits $\mathfrak{A}$. If $\mathfrak{K}_0(z)$ has degree $2n$ over $\mathfrak{K}_0$ and $\mathfrak{K}(z)$ has degree n over $\mathfrak{K}$ then we have proved in Section 9 that $\mathfrak{A}$ is similar to a cyclic algebra of type B. Hence let the degree of $Z_0 = \mathfrak{K}_0(z)$ over $\mathfrak{K}_0$ be the degree of $Z = \mathfrak{K}(z)$ over $\mathfrak{K}$ so that $Z = Z_0 \times \mathfrak{K}$. But Z_0 is cyclic over $\mathfrak{K}$ and hence $\mathfrak{A}$ is similar to a cyclic algebra of type A. We have

THEOREM 19. *Every J-involutorial simple algebra over an infinite reduced field $\mathfrak{F}$ is either similar to an algebra of type* A *or one of type* B.

11. **Transcendental extensions of $\mathfrak{F}$.** We have proved that the structure of a J-involutorial simple algebra $\mathfrak{A} = \mathfrak{B}_{\mathfrak{F}}$ is determined by that of $\mathfrak{B}$ where $\mathfrak{B}$ is a linear sub-set of $\mathfrak{A}$ over a reduced sub-field $\mathfrak{F}_0$ of $\mathfrak{F}$ and $\mathfrak{B}$ is a J-involutorial simple algebra over $\mathfrak{F}_0$. We may obtain a simpler treatment however by extending $\mathfrak{F}$ to a field $\mathfrak{H} = \mathfrak{F}(\xi)$ where ξ is an indeterminate. We are of course assuming that $\mathfrak{F}$ is infinite so that $\mathfrak{H}$ is an H.I. field and every J-involutorial simple

[35] Albert (12), (16), (13).

algebra over $\mathfrak{H}$ is similar to an algebra of type A. We consider of course only the case $\mathfrak{K} \neq \mathfrak{K}_0$ by Theorem 12.

Without loss of generality we consider a division algebra $\mathfrak{D}$ over $\mathfrak{F}$ and let $\mathfrak{C} = \mathfrak{D}_{\mathfrak{H}}$. Then $\mathfrak{C}$ is a division algebra. For otherwise $ab = 0$ for a and b in $\mathfrak{C}$ and both not zero. By multiplying a and b by properly chosen quantities of $\mathfrak{H}$ we may assme that both are polynomials in ξ with coefficients in $\mathfrak{F}$ and constant terms $a_0 \neq 0$, $b_0 \neq 0$ in $\mathfrak{D}$. Then $a_0 b_0 = 0$ which is impossible.

We seek necessary and sufficient conditions on $\mathfrak{C}$ that $\mathfrak{D}$ with J-involutorial centrum $\mathfrak{K} = \mathfrak{K}_0(q)$ shall be J-involutorial. If $\mathfrak{D}$ is J-involutorial then so obviously is $\mathfrak{C}$ with centrum. $\mathfrak{K}_2 = \mathfrak{K}_1(q)$, $\mathfrak{K}_1 = \mathfrak{K}_0(q)$. The J-centrum preserving involutions of $\mathfrak{C}$ are correspondences T given by

$$c^T = p^{-1} c^J p \qquad (c \text{ in } \mathfrak{C}),$$

where $p = \pm p^J$ is in $\mathfrak{C}$. Thus $\mathfrak{C}$ may be T-involutorial and yet T may not be an involution of $\mathfrak{D}$. However we may prove

THEOREM 20. *Let $\mathfrak{D}$ be a division algebra over its J-involutorial centrum $\mathfrak{K} = \mathfrak{K}_0(q)$ and let $\mathfrak{C} = \mathfrak{D}_{\mathfrak{H}}$ be J-involutorial of the second kind over $\mathfrak{H}$ such that the involution J in $\mathfrak{K}$ is preserved. Then there exists a J-centrum preserving involution T of $\mathfrak{C}$ such that T is an involution of $\mathfrak{D}$.*

For let $u_1, \cdots, u_r$ be a basis of $\mathfrak{D}$ over $\mathfrak{F}$ and suppose that $\mathfrak{C}$ is J-involutorial over $\mathfrak{H}$. Then $u_i u_j = \Sigma \gamma_{ijk} u_k$ with γ_{ijk} in $\mathfrak{F}$ so that

$$u_j^J\, u_i^J = \Sigma \gamma_{ijk}\, u_k^J \tag{32}$$

identically in the indeterminate ξ. We may write

$$u_i^J = [\delta(\xi)]^{-1} \sum_j a_{ij}(\xi) u_j\,, \tag{33}$$

where the $a_{ij}(\xi)$ and $\delta(\xi)$ are polynomials in ξ with coefficients in $\mathfrak{F}_j$ and no irreducible factor of $\delta(\xi)$ divides all the $a_{ij}(\xi)$. We are also assuming that

$$k_0^J = k_0\,, \qquad q^J = -q \text{ or } q + 1\,,$$

according as $\mathfrak{F}$ does not or does have characteristic two.

If $\delta(0) = 0$ then δ has ξ as a factor and at least one $a_{ij}(\xi)$ does not have ξ as a factor. For this i we have $\delta(\xi) u_i^J$ different from zero when we replace ξ by zero. But (32) for $j = i$ gives

$$\begin{aligned}[][\delta(\xi) u_i^J]^2 &= \delta(\xi) \sum_k \gamma_{iik} [\delta(\xi) u_k^J] \\ &= \delta(\xi) \sum_k \gamma_{iik} \sum_t a_{kt}(\xi) u_j\,,\end{aligned}$$

which vanishes at $\xi = 0$, so that $u_{0i} = \delta(0) u_i^J(0) \neq 0$ is in $\mathfrak{D}$, and $u_{0\,i}^2 = 0$. This is impossible. Hence $\delta(0) \neq 0$. Define

$$u_i^T = [\delta(0)]^{-1} \sum_j a_{ij}(0) u_j\,, \tag{34}$$

and obtain $u_j^T u_i^T = \Sigma\gamma_{ijk}u_k^T$. Moreover

$$u_i \equiv \delta(\xi)^{-1}\,\Sigma\, a_{ij}(\xi)u_j^J \tag{35}$$

identically in ξ, so that $u_i = \delta(0)^{-1}\,\Sigma\, a_{ij}(0)\; u_j^T = (u_i^T)^T$. It is obvious that $k_0^T = k_0$, $q^T = q^J$ so that T is a J-centrum preserving involution of both $\mathfrak{C}$ and $\mathfrak{D}$.

12. **Division algebras over an algebraic number field.** We shall consider the case where $\mathfrak{F}$ is an algebraic number field of finite degree over the rational number field $\mathfrak{R}$. By passing to an algebra equivalent to $\mathfrak{D}$ we may obviously take $\mathfrak{K}$ to be an algebraic number field of finite degree over $\mathfrak{R}$. I have proved[36]

THEOREM A. *A division algebra $\mathfrak{D}$ over $\mathfrak{K}$ has exponent two if and only if its degree is two.*

The above result combined with Theorem 12 evidently determines all J-involutorial division algebras $\mathfrak{D}$ of the first kind. We have

$$\mathfrak{D} = (1, i, j, ij)\,, \qquad i^2 = \alpha\,, \qquad j^2 = \beta\,, \qquad ji = -ij(\alpha, \beta \text{ in } \mathfrak{K})\;; \tag{36}$$

with J given by

$$i^J = i\,, \qquad j^J = j\,, \qquad (ij)^J = -\,ij\,. \tag{37}$$

We may easily determine all J-centrum preserving involutions of $\mathfrak{D}$. For let T be such an involution so that by Theorem 4 and by (37) we have

$$i^T = p^{-1}ip\,, \qquad j^T = p^{-1}jp\,, \qquad p^J = \pm\, p\,.$$

Let first $p^J = -\,p$ so that $p = \rho ij$ with $\rho \neq 0$ in $\mathfrak{K}$. Then $p^{-1} = -\,i$, $p^{-1}jp = -\,j$ and

$$i^T = -\,i\,, \qquad j^T = -\,j\,, \qquad (ij)^T = -\,ij\,,$$

for this case.

Let next $p^J = p$ so that $p = \delta + i_0$ where $i_0 = \mu i + \nu j = i_0^J$ and δ, μ, ν are in $\mathfrak{K}$. If $i_0 = 0$ then p is in $\mathfrak{K}$ and $i^T = i, j^T = j$. Let $i_0 \neq 0$ so that i_0 is not in $\mathfrak{K}$ but $i_0^2 = \alpha_0 = \mu^2\alpha + \nu^2\beta$ is in $\mathfrak{K}$. Then $i_0^T = p^{-1}i_0^J p = p^{-1}(p - \delta)p = p - \delta = i_0$. We also have $(ij)i_0 = -\,i_0(ij)$ and hence $j_0 i_0 = -\,i_0 j_0$ if $j_0 = i_0(\delta - i_0)ij, j_0^2 = \beta_0 = \alpha_0(\lambda^2 - \alpha_0)\alpha\beta$. But

$$j_0^T = p^{-1}(-ij)i_0(\delta - i_0)p = p^{-1}i_0(\delta + i_0)(ij)p = i_0(ij)(\delta + i_0)$$
$$= i_0(\delta - i_0)ij = j_0\,.$$

We may then take $1, i_0, j_0, i_0j_0$ as a *new basis* of $\mathfrak{D}$ with (37) holding. We have proved

THEOREM 21. *Let $\mathfrak{D} \neq \mathfrak{K}$ be a J-involutorial division algebra of the first kind over $\mathfrak{K}$. Then if T is any J-centrum preserving involution of $\mathfrak{D}$ a basis* $1, i, j, ij$

[36] Albert (3).

may be so chosen that $i^2 = \alpha$ *in* $\mathfrak{K}$, $j^2 = \beta$ *in* $\mathfrak{K}$, $ji = -ij$ *and either*

$$i^T = i\,, \qquad j^T = j\,, \qquad (ij)^T = -ij \tag{38}$$

or

$$i^T = -i\,, \qquad j^T = -j\,, \qquad (ij)^T = -ij\,. \tag{39}$$

Algebras of the second kind have a much more complicated structure but we shall prove, for the case where $\mathfrak{K}$ is a finite algebraic extension of $\mathfrak{R}$,

THEOREM 22. *A division algebra* $\mathfrak{D}$ *is J-involutorial of the second kind if and only if* $\mathfrak{D}$ *is a cyclic algebra of type* A.

We shall take $\mathfrak{K}$ to be an algebraic number field and, by Theorems 10 and 13, need only prove that there is a cyclic field Z_0 of degree n over $\mathfrak{K}_0$ such that $(Z_0, \mathfrak{K})$ splits $\mathfrak{D}$. For then $(Z_0, \mathfrak{K})$ will have degree n over $\mathfrak{K}$.

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{K}$, $\mathfrak{K}_\mathfrak{p}$ the $\mathfrak{p}$-adic extension of $\mathfrak{K}$. If Z is a cyclic field over $\mathfrak{K}$ and $\mathfrak{P}$ a prime divisor in Z of $\mathfrak{p}$ then it is well known that $Z_\mathfrak{P}$ is the composite of Z and $\mathfrak{K}_\mathfrak{p}$. Thus the degree of $Z_\mathfrak{P}$ over $\mathfrak{K}_\mathfrak{p}$ is an integer $r_\mathfrak{p}$ independent of $\mathfrak{P}$ and is called the $\mathfrak{p}$-degree of Z.

Let $\mathfrak{D}$ be a normal division algebra over $\mathfrak{K}$ and $\mathfrak{D}_\mathfrak{p}$ the algebra obtained by extending the centrum of $\mathfrak{D}$ to $\mathfrak{K}_\mathfrak{p}$. Then $\mathfrak{D}_\mathfrak{p}$ is a normal simple algebra whose index $m_\mathfrak{p}$ is called the $\mathfrak{p}$-index of $\mathfrak{D}$.

The field $\mathfrak{K}$ has degree t over the field of all rational numbers and has algebraic number conjugates $\mathfrak{K}_1, \cdots, \mathfrak{K}_t$. Let Z be cyclic of degree n over $\mathfrak{K}$ and consider the field Z_i over $\mathfrak{K}_i$ equivalent to Z over $\mathfrak{K}$ and the algebras $\mathfrak{D}_i$ over $\mathfrak{K}_i$ equivalent to $\mathfrak{D}$ over $\mathfrak{K}$.

If $\mathfrak{R}$ is the field of all real numbers, and $\mathfrak{R}_i$ is the composite of $\mathfrak{R}$ and $\mathfrak{K}_i$, then $\mathfrak{R}_i$ is the field of all real numbers or all complex numbers according as $\mathfrak{K}_i$ is or is not real. The composite $(Z_i, \mathfrak{R})$ has degree $r_i = 1, 2$ over $\mathfrak{R}_i$, the $\mathfrak{K}_i$*-degree* of Z. The algebra $\mathfrak{D}_{i\mathfrak{R}_i}$ over $\mathfrak{R}_i$ has index $m_i = 1, 2$, the $\mathfrak{K}_i$*-index* of $\mathfrak{D}$. H. Hasse has then given the following arithmetic criteria.[37]

LEMMA H1. *Let* $\mathfrak{D}$ *be a normal division algebra of degree* n *over its* $\mathfrak{p}$*-adic centrum* $\mathfrak{K}_\mathfrak{p}$ *and* Z *be a cyclic extension of* $\mathfrak{K}_\mathfrak{p}$. *Then* Z *splits* $\mathfrak{D}$ *if and only if the degree of* Z *over* $\mathfrak{K}_\mathfrak{p}$ *is a multiple of* n.

LEMMA H2. *A cyclic field* Z *over* $\mathfrak{K}$ *is a splitting field of division algebra* $\mathfrak{D}$ *over its centrum* $\mathfrak{K}$ *if and only if the* $\mathfrak{p}$*-degrees and* $\mathfrak{K}_i$*-degrees of* Z *are multiples of the corresponding indices of* $\mathfrak{D}$.

LEMMA H3. *The* $\mathfrak{p}$*-indices of* $\mathfrak{D}$ *are unity except for a finite number of prime ideals* $\mathfrak{p}$ *of* $\mathfrak{K}$.

We shall also use the Grünwald theorem[38]

LEMMA G4. *Let* $p_1, \cdots, p_r$ *be prime ideals of* $\mathfrak{K}$, n *an integer*, $\mathfrak{K}_1, \cdots, \mathfrak{K}_s$ *a*

[37] H. Hasse (1), (2), (4).

[38] See the table of literature. We have used Grünwald's Theorem 3 with $e_k = 1, f_k = n$ for the prime ideals $\mathfrak{p}_k$ and with $e_k = 2, f_k = d_k = 1$ for the infinite $\mathfrak{p}_k$, that is for our $\mathfrak{K}_i$. It is well known that Z has $\mathfrak{p}_i$ degree $e_i f_i$.

set of real conjugates of $\mathfrak{K}$. *Then there exists a cyclic field* Z *of degree* n *over* $\mathfrak{K}$ *with* $\mathfrak{p}_j$*-degrees* n *and* $\mathfrak{K}_i$*-degrees* $2, j = 1, \cdots, r, i = 1, \cdots, s$.

We now consider the case where $\mathfrak{D}$ has degree two over $\mathfrak{K} = \mathfrak{K}_0(q)$. Then some x of $\mathfrak{D}$ is not in $\mathfrak{K}$ so that one of $x + x^J$ and $(x - x^J)q$ is not in $\mathfrak{K}$. Since both quantities are J-symmetric we have proved the existence of a J-symmetric quantity i of $\mathfrak{D}$ and not in $\mathfrak{K}$.

The minimum equation of i has coefficients in $\mathfrak{K}_0$ and degree two. We may obviously take this equation to be reduced, $i^2 = \alpha$ in $\mathfrak{K}_0$. Then there exists a quantity j_0 in $\mathfrak{D}$ such that $j_0^i = -ij_0$ and $1, i, j_0, i_0j_0$ form a basis of $\mathfrak{D}$ over $\mathfrak{K}$. But then $ij_0^J = -j_0^Ji$. If $j_0 + j_0^J \neq 0$ then we put $j = j_0 + j_0^J = j^J$. If $j_0^J = j_0$ then put $j = qj_0 = j^J$. In either case $1, i, j, ij$ form a basis of $\mathfrak{D}$ such that $i^J = i, j^J = j, ji = -ij$ while $i^2 = \alpha = \alpha^J$ in $\mathfrak{K}_0$, $j^2 = \beta = \beta^J$ in $\mathfrak{K}_0$. We have proved

LEMMA 5. *Let* $\mathfrak{D}$ *be* J*-involutorial of degree two over its centrum* $\mathfrak{K} = \mathfrak{K}_0(q)$, $q^J = -q$. *Then* $\mathfrak{D}$ *is an algebra of type* A *and in fact* $\mathfrak{D} = \mathfrak{D}_0 \times \mathfrak{K}(q)$,

$$\mathfrak{D}_0 = (1, i, j, ij), \quad i^2 = \alpha, \quad j^2 = \beta, \quad ji = -ij$$

over $\mathfrak{K}_0$, *and* $i^J = i, j^J = j = \beta j^{-1}$.

We now let $\mathfrak{D}$ be J-involutorial of degree n over its centrum $\mathfrak{K} = \mathfrak{K}_0(q)$, $q^J = -q$ and let $\pi_1, \cdots, \pi_r$ be the prime ideals of $\mathfrak{K}$ for which $\mathfrak{D}$ has π-index not unity. Suppose also that $\mathfrak{K}_{01}, \cdots, \mathfrak{K}_{0\mu}$ are the real conjugates of $\mathfrak{K}_0$ for which the corresponding $\mathfrak{K}_i$ are real and $\mathfrak{D}_i$ over $\mathfrak{K}_i$ has index two. By Lemma G4 there exists a cyclic field Z_0 of degree n over $\mathfrak{K}_0$ with $\mathfrak{K}_{0i}$-degrees two and $\mathfrak{p}_j$ degrees n where $\mathfrak{p}_j$ in $\mathfrak{K}_0$ has π_j as prime ideal factor in $\mathfrak{K}$. We shall prove that the composite Z of Z_0 and $\mathfrak{K}$ splits $\mathfrak{D}$ and hence have Theorem 22.

We shall use the trivial consequence of Theorem 9 given before:

LEMMA 6. *Let* Y, Z *be algebraic extönsions of degree two,* n *respectively of a field* $\mathfrak{K}$. *Then* (Y, Z) *has degree* n *or* $n/2$ *over* Y *according as* Z *does not or does have a sub-field equivalent to* Y.

We write $n = 2^e n_0 = 2\nu$ where n_0 is odd and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{K}_0$ such that the corresponding π-index of $\mathfrak{D}$ is divisible by 2^e. Then $\mathfrak{D}_\pi$ is the direct product of a total matric algebra of odd order and a division algebra $\mathfrak{B}$ over $\mathfrak{K}_\pi$ whose exponent is its degree m_π. The algebra $\mathfrak{D}^\nu = M \times Q$ where M is total matrix and Q has degree two over $\mathfrak{K}$. By Theorem 4 Q is J-involutorial and hence $Q = Q_0 \times \mathfrak{K}$ where Q_0 is J-involutorial over $\mathfrak{K}_0$ by Lemma 5.

We obviously have $\mathfrak{D}_\pi^\nu = M \times Q_\pi$. By hypothesis the exponent of $\mathfrak{D}_\pi$ is divisible by 2^e so that Q_π must be a division algebra. But $Q_\pi = Q_{0\mathfrak{p}} \times \mathfrak{K}_\pi$. By Lemma H1 the field $\mathfrak{K}_\pi = (\mathfrak{K}_{0\mathfrak{p}}, \mathfrak{K})$ must have degree unity over $\mathfrak{K}_{0\mathfrak{p}}$. But then the composite $(Z, \mathfrak{K}_\pi)$ of $(Z_0, \mathfrak{K}_{0\mathfrak{p}})$ and $\mathfrak{K}_\pi$ has degree n over $\mathfrak{K}_\pi$ since $(Z_0, \mathfrak{K}_{0\mathfrak{p}})$ has degree n over $\mathfrak{K}_{0\mathfrak{p}}$ and $\mathfrak{K}_\pi$ has degree unity over $\mathfrak{K}_{0\mathfrak{p}}$. Hence the π-degree of Z is n for every π such that the π-index of $\mathfrak{D}$ is divisible by 2^e.

Let next $\mathfrak{D}$ have π-index $m \neq 1$ such that 2^e does not divide m_π. Since m_π divides n we have m_π a divisor of ν. The π-degree of $Z = (Z_0, \mathfrak{K})$ is a multiple of ν since $(Z_0, \mathfrak{K}_{0\mathfrak{p}})$ has degree n over $\mathfrak{K}_{0\mathfrak{p}}$, $\mathfrak{K}_\pi = (\mathfrak{K}_{0\mathfrak{p}}, \mathfrak{K})$ has degree one or two

over $\mathfrak{K}_{0\mathfrak{p}}$ and we may apply Lemma 6. Our construction of Z_0 implies that Z has $\mathfrak{K}_i$-degrees two wherever $\mathfrak{D}$ has $\mathfrak{K}_i$ index two and hence Z splits $\mathfrak{D}$ by Lemma H2.

13. **Algebras of Riemann matrices.** If ω is a pure Riemann matrix of the second kind its multiplication algebra is a J-involutorial division algebra $\mathfrak{D}$ over the rational number field. Then $\mathfrak{K} = \mathfrak{K}_0(q)$ where $\mathfrak{K}_0$ is total real (has all real conjugates) and $q^2 = \mu$ is total negative. The fields $\mathfrak{K}_i$ are all imaginary and $\mathfrak{D}$ has $\mathfrak{K}_i$ indices unity. In this case we may prove the important[39]

THEOREM 23. *The multiplication algebra of a Riemann matrix of the second kind is an algebra of type* A *generated by* $Z = (Z_0, \mathfrak{K})$ *where* Z_0 *is a total real cyclic field over* $\mathfrak{K}_0$.

For let the prime ideals $\mathfrak{p}_j$ be defined as in the proof of Theorem 23 and use Lemma G4 to prove the existence of a cyclic field W_0 of degree $2n$ over $\mathfrak{K}_0$ and $\mathfrak{p}_i$-degrees $2n$. The field W_0 has a cyclic sub-field Z_0 of degree n over $\mathfrak{K}_0$ and $\mathfrak{p}_i$-degrees n, and $Z = (Z_0, \mathfrak{K})$ splits $\mathfrak{D}$ by the proof of Theorem 23. Moreover Z_0 is total real since we have

LEMMA 7. *Let* $\mathfrak{F}$ *be a real field,* W *be cyclic of degree* t *over* $\mathfrak{F}$. *Then either* W *is real or* $t = 2n$ *and* W *has a real cyclic sub-field of degree* n *over* $\mathfrak{F}$.

For the conjugate fields of W are equal to W and hence W contains its complex conjugate. If T is the automorphism of W carrying each quantity to its complex conjugate then T^2 is the identity automorphism I. Hence $T = I$ and W is real or (I, T) is the unique sub-group of order two of the cyclic group of W. Then W has degree $t = 2n$ and the field Z of all quantities of W unaltered by T is real and cyclic of degree n over $\mathfrak{K}$.

III. THE MULTIPLICATION ALGEBRAS OF WEYL MATRICES

1. **Weyl Matrices.** Let Γ be a J-involutorial field containing the least algebraically closed extension Λ of a field $\mathfrak{F}$ and assume that α^J is in $\mathfrak{F}$ for every α in $\mathfrak{F}$.

The quantities of Λ are algebraic of finite degree over $\mathfrak{F}$. If

$$\xi^t + \alpha_1\xi^{t-1} + \cdots + \alpha_t = 0$$

with α_i in $\mathfrak{F}$ then ξ is in Λ and $(\xi^J)^t + \alpha_1^J(\xi^J)^{t-1} + \cdots + \alpha_t^J = 0$ so that ξ^J is algebraic of finite degree over $\mathfrak{F}$. Hence ξ^J is in Λ for every ξ in Λ.

Let $\Gamma_0, \Lambda_0, \mathfrak{F}_0$ be the sets of all J-symmetric quantities of $\Gamma, \Lambda, \mathfrak{F}$ respectively. Then $\Gamma_0, \Lambda_0, \mathfrak{F}_0$ are fields and $\Gamma_0 \geqq \Lambda_0 \geqq \mathfrak{F}_0$. If $\Lambda \neq \Lambda_0$ then $\Lambda = \Lambda_0(q)$, $q^J = -q$, $q^2 = \mu$ in Λ_0. We then have the Artin-Schreier[40]

---

[39] The present proof is much simpler than that in Albert (5). Moreover the existence proof for Z_0 had an hiatus in the part where the author showed that Z_0 could be taken total real. This is corrected by the simple device used to prove the above Theorem 23.

[40] A field Λ_0 is said to be real if -1 is not a sum of squares in Λ_0. Moreover Λ_0 is real closed if no proper algebraic extension of Λ_0 is real. The field Λ_0 then has a unique ordering and most of the theorems of ordinary real algebra hold in Λ_0. See Artin-Schreier (1), (2).

THEOREM 24. *Let $\Lambda = \Lambda_0(q) \neq \Lambda$. Then Λ_0 is a real closed field of characteristic zero, $\Lambda = \Lambda_0(i), i^2 = -1$.*

The algebra $\mathfrak{M}$ of all p-rowed square matrices with elements in Γ is a J-involutorial simple algebra with J given by

$$\tau = (\tau_{ij}), \qquad \tau^J = (\sigma_{ij}), \qquad \sigma_{ij} = \tau^J_{ji} \qquad (i, j = 1, \cdots, p). \tag{40}$$

Consider in particular a J-symmetric matrix

$$\tau = RC, \tag{41}$$

where C has elements in $\mathfrak{F}$ and

$$C^J = \epsilon C, \qquad \epsilon = \pm 1. \tag{42}$$

Suppose also that τ is totally regular in Λ, that is every principal minor of $V\tau V^J$ is non-singular for any non-singular V with elements in Λ. Then we shall call R a *Weyl matrix*[41] over $\mathfrak{F}$ with principal matrix C. If U is any non-singular matrix with elements in $\mathfrak{F}$ then

$$R_U = URU^{-1} \tag{43}$$

is a Weyl matrix isomorphic to R. For obviously

$$\tau_U = U\tau U^J = (URU^{-1})UCU^J = R_U C_U \tag{44}$$

with $\tau_U = \tau_U^J$ totally regular and $C_U^J = \epsilon C_U$.

If G and H are non-singular matrices with elements in $\mathfrak{F}$ such that GRH is a Weyl matrix then we shall say that GRH is *associated* with R. Evidently *τ is associated with R.*

The set $\mathfrak{A}$ of all p-rowed square matrices A with elements in $\mathfrak{F}$ such that

$$AR = RA \tag{45}$$

is a linear associative algebra over $\mathfrak{F}$ called the *multiplication algebra* of R. We shall study the structure of $\mathfrak{A}$.

2. **The reduction theory.** A Weyl matrix R is called reducible if it is isomorphic to

$$\begin{pmatrix} R_1 & Q \\ 0 & R_2 \end{pmatrix}, \tag{46}$$

where R_1 has $m < p$ rows and columns; otherwise irreducible. If we write

$$\tau = \begin{pmatrix} \tau_1 & \tau_3 \\ \tau_4 & \tau_2 \end{pmatrix} = RC = \begin{pmatrix} R_1 & Q \\ 0 & R_2 \end{pmatrix}\begin{pmatrix} C_1 & C_3 \\ C_4 & C_2 \end{pmatrix} \tag{47}$$

then

$$\tau_2 = R_2C_2, \qquad \tau_4 = R_2C_4, \qquad \tau_3 = R_1C_3 + QC_2. \tag{48}$$

[41] See Weyl (2). Weyl considered the case where Γ is the field of all complex numbers, τ is real, and wrote $\tau = CR$. It is more natural to take our equivalent form $\tau = RC$ above and our later theory of Chapter IV is simplified thereby.

Since τ is totally regular τ_2 and hence C_2 are non-singular. By a simple computation we have the[42]

POINCARÉ THEOREM. *A reducible Weyl matrix* (46) *is isomorphic to*

$$R_U = URU^{-1} = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}, \tag{49}$$

where R_1 and R_2 are Weyl matrices and

$$U = \begin{pmatrix} I_m & B \\ 0 & I_{p-m} \end{pmatrix}, \qquad B = -C_3C_2^{-1}. \tag{50}$$

As an immediate consequence of the Poincaré theorem any Weyl matrix R is isomorphic to

$$\begin{pmatrix} S_1 & & \\ & \ddots & \\ & & S_t \end{pmatrix}, \qquad S_j = \begin{pmatrix} R_{j1} & & \\ & \ddots & \\ & & R_{jt_j} \end{pmatrix}, \qquad R_{jk} = R_j, \tag{51}$$

with R_j irreducible and R_k not isomorphic to R_j for $j \neq k$. We also have the[43]

SCHUR LEMMA. *Let R_1 and R_2 be irreducible Weyl matrices and $UR_1 = R_2U$ for U in $\mathfrak{F}$. Then $U = 0$ or is non-singular.*

It is now easily shown that algebra $\mathfrak{A}$ is a semi-simple algebra with simple components $\mathfrak{A}_j$, the multiplication algebras of the S_j. Each $\mathfrak{A}_j = \mathfrak{M}_j \times \mathfrak{D}_j$ where $\mathfrak{D}_j$ is the multiplication algebra of R_j and is a division algebra, $\mathfrak{M}_j$ is a total matric algebra of degree t_j. This than reduces the study of $\mathfrak{A}$ to the case where R is irreducible and $\mathfrak{A} = \mathfrak{D}$, a division algebra.

3. Weyl matrices over a modular field.

The multiplication algebra $\mathfrak{A}$ of a Weyl matrix R over $\mathfrak{F}$ is an involutorial algebra over $\mathfrak{F}$. For let $\tau = RC = \tau^J = C^JR^J = \epsilon CR^J$ and $AR = RA$. Then $A^JR^J = R^J(\epsilon C^{-1}RC) = \epsilon(C^{-1}RC)A^J$ and hence $CA^JC^{-1}R = R(CA^JC^{-1})$,

$$A^T = CA^JC^{-1} \tag{52}$$

is in $\mathfrak{A}$ for every A of $\mathfrak{A}$.

We assume now that $\mathfrak{F}$ has characteristic $p > 0$. By Theorem 24, $\Lambda = \Lambda_0$ is composed of J-symmetric quantities so that A^J is the transpose A' of A. Then

$$A^T = CA'C^{-1}, \qquad A' = RCA' = RA^TC = A^T \tag{53}$$

for every A of $\mathfrak{A}$. We shall prove

LEMMA 1. *Let $A = A^T$ be in $\mathfrak{A}$. Then the algebra $\Lambda(A)$ contains no nilpotent matrix.*

---

[42] Cf. Weyl (loc. cit.) for the case $\tau = CR$. His proof is almost identical with ours except that we have $C^J = \epsilon C$, $\epsilon = \pm 1$ instead of $\epsilon = -1$. Hence we shall give no details here.

[43] Cf. Wedderburn (4), section 8.04.

For if $B \neq 0$ is in $\Lambda(A)$ and is nilpotent we may take $B^2 = 0$, $B \neq 0$, without loss of generality. But $\tau A' = A\tau$ so that $\tau(A')^k = A^k\tau$ and $\tau B' = B\tau$. It is well known that there exists a non-singular matrix G with elements in Λ such that

$$B_0 = GBG^{-1} = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \tag{54}$$

We write

$$\tau_0 = G\tau G' = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_3 & \tau_4 \end{pmatrix}, \qquad B_0\tau_0 = \begin{pmatrix} B_1\tau_1 & B_1\tau_2 \\ B_2\tau_3 & B_2\tau_4 \end{pmatrix} = \tau_0 B_0' = \begin{pmatrix} \tau_1 B_1' & \tau_2 B_2' \\ \tau_3 B_1' & \tau_1 B_2' \end{pmatrix}, \tag{55}$$

where τ_1 is a square matrix of two rows, and obtain $B_1\tau_1 = \tau_1 B_1'$,

$$\tau_1 = \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}, \qquad B_1\tau_1 = \begin{pmatrix} \lambda_3 & \lambda_4 \\ 0 & 0 \end{pmatrix} = \tau_1 B_1' = \begin{pmatrix} \lambda_2 & 0 \\ \lambda_4 & 0 \end{pmatrix}, \tag{56}$$

so that $\lambda_4 = 0$. But τ is totally regular in Λ and so is τ_0 which has $\lambda_4 = 0$ as principal minor, a contradiction.

If $\mathfrak{F}(A)$ is a field which is inseparable over $\mathfrak{F}$ then $\Lambda(A)$ contains a nilpotent matrix.[44] Hence we have

LEMMA 2. *Let $\mathfrak{F}(A)$ be a field and $A = A^T$. Then $\mathfrak{F}(A)$ is separable over $\mathfrak{F}$.*

We now assume that $\mathfrak{F}(A)$ is a field and A^T is in $\mathfrak{F}(A)$. Then the field $\mathfrak{F}(A)$ is a J-involutorial division algebra so that either $A = A^J$ or $\mathfrak{F}(A) = \mathfrak{K}_0(q)$ where $q^J = -q$ or $q + 1$. In any case $\mathfrak{K}_0$ is separable over $\mathfrak{F}$, $\mathfrak{K}_0(q)$ is separable over $\mathfrak{K}_0$, so that $\mathfrak{F}(A)$ is separable over $\mathfrak{F}$. Hence the roots $\alpha_1, \cdots, \alpha_t$ of the minimum equation of A are all distinct and $p = tr$,

$$V = (\alpha_j^{k-1} I_r) \qquad (j, k = 1, \cdots, t), \tag{57}$$

is non-singular. We may take A so that

$$\alpha = VAV^{-1} = \begin{pmatrix} \alpha_1 I_r & & \\ & \ddots & \\ & & \alpha_t I_r \end{pmatrix}. \tag{58}$$

Then $V^J = V'$ and $V\tau V' = VRV^{-1}VCV'$ has non-singular principal minors. Put $VCV' = (C_{jk})$ and $CA'C^{-1} = A^T = f(A)$, so that $(VCV')(VAV^{-1})' = Vf(A)V^{-1}VCV'$ and hence

$$C_{jk}[\alpha_k - f(\alpha_j)] = 0 \qquad (j, k = 1, \cdots, t). \tag{59}$$

It follows that

$$C_{jk} = 0 \qquad (\alpha_k \neq f(\alpha_j)). \tag{60}$$

[44] Cf. Van der Waerden, vol. II, p. 174.

Since $AR = RA$ the matrix α is commutative with VRV^{-1} and hence

$$VRV^{-1} = \begin{pmatrix} R_1 & & \\ & \ddots & \\ & & R_t \end{pmatrix}.$$

Then

$$VTV' = (R_j C_{jk}) \tag{61}$$

has non-singular principal minors, so that C_{jj} is non-singular. But $C_{jj} = 0$ unless $\alpha_j = f(\alpha_j)$. Hence $f(A) \equiv A$. We have proved

LEMMA 3. *Let A^T be in the field $\mathfrak{F}(A)$. Then $A^T = A$.*

Suppose that $\mathfrak{F}$ has characteristic two and let $\mathfrak{D}$ be a normal division algebra over $\mathfrak{F}$ such that $\mathfrak{D} \leqq \mathfrak{A}$ and A^T is in $\mathfrak{D}$ for every A of $\mathfrak{D}$. If $\mathfrak{C}$ is any T-involutorial sub-field of $\mathfrak{D}$ then we have proved that either $\mathfrak{C} = \mathfrak{C}_0$ is composed of T-symmetric quantities or $\mathfrak{C} = \mathfrak{C}_0(q)$ is a separable extension of $\mathfrak{C}_0$. By Lemma 2 the field $\mathfrak{C}_0$ is separable over $\mathfrak{F}$ and hence $\mathfrak{C}$ is separable over $\mathfrak{F}$. But by Lemma 3 we have $\mathfrak{C} = \mathfrak{C}_0$. We assume that $\mathfrak{C}$ has the largest degree of all symmetric sub-fields of $\mathfrak{D}$ and hence $\mathfrak{C} = \mathfrak{F}(A)$. The algebra $\mathfrak{B}$ of all quantities of $\mathfrak{D}$ commutative with A is a normal division algebra over $\mathfrak{F}(A)$ and contains no $B = B^T$ not in $\mathfrak{F}(A)$. But if B is in $\mathfrak{B}$ then $BA = AB$, $AB^J = B^J A$ and B^J is in $\mathfrak{B}$. When $\mathfrak{B} \neq \mathfrak{F}(A)$ there exists a $B \neq B^J$ in B, while $\beta = B + B^J$ is in $\mathfrak{F}(A)$, and $B^J = \beta - B$ is in $\mathfrak{F}(B, A)$. Hence $\mathfrak{F}(B, A)$ is a T-involutorial sub-field of $\mathfrak{D}$ and $B^J \neq B$, a contradiction. Thus $\mathfrak{B} = \mathfrak{F}(A)$.

Algebra $\mathfrak{D}$ has degree 2^e over $\mathfrak{F}$ by Theorem 12 and $\mathfrak{F}(A)$ is a maximal sub-field of $\mathfrak{D}$. It is known[45] that then there is a field $\mathfrak{F}_1 < \Lambda$ such that $\mathfrak{D}_{\mathfrak{F}_1} = \mathfrak{D} \times \mathfrak{F}_1$, is a T-involutorial normal division algebra over $\mathfrak{F}_1$ and the field $\mathfrak{F}_1(A)$ contains a subfield $\mathfrak{F}_1(A_0)$ of degree 2^{e-1} over $\mathfrak{F}_1$. The algebra $\mathfrak{B}$ of all quantities of $\mathfrak{D}_{\mathfrak{F}_1}$ commutative with A_0 is a normal division algebra of degree two over $\mathfrak{H} = \mathfrak{F}_1(A_0)$ and contains the separable quadratic extension $\mathfrak{H}(A) = \mathfrak{F}_1(A)$ of $\mathfrak{H}$. We may write $\mathfrak{H}(A) = \mathfrak{H}(A_1)$ where $A_1^2 = A_1 + \alpha$ and α is in $\mathfrak{H}$. Then there exists a B in $\mathfrak{B}$ such that $BA = (A + 1)B$. But $B(A + 1) = (A + 1)B + B = AB$ and $B^T A = (A + 1)B^T$ so that $(B + B^T)A = (A + 1)(B + B^T)$. We may take $B = B^T$ without loss of generality since B^T is in $\mathfrak{B}$ and either $B = B^T$ or $B + B^T \neq 0$ transforms A into $A + 1$. But then $B^2 A = AB^2$ and $B^2 = \beta$ is in $\mathfrak{H}$. Since B is not in $\mathfrak{H}$ the T-symmetric field $\mathfrak{H}(B)$ is inseparable over $\mathfrak{H}$ and hence over $\mathfrak{F}$. This is impossible by Lemma 2 so that $e = 0$ and $\mathfrak{D} = \mathfrak{F}$.

We now let $\mathfrak{D}$ be the multiplication algebra of any irreducible Weyl matrix over a field $\mathfrak{F}$ of characteristic $\pi > 0$. If $\mathfrak{D}$ contains only T-symmetric quantities then by the first section of Chapter II algebra $\mathfrak{D} = \mathfrak{K}_0$ is a T-symmetric field. If $\pi \neq 2$ and $\mathfrak{D} \neq \mathfrak{K}_0$ then there exists an $A \neq A^T$ in $\mathfrak{D}$ so that $B = A - A^T \neq 0$ and $B^T = -B$ contrary to Lemma 3. Hence again $\mathfrak{D} = \mathfrak{K}_0$. Thus

[45] Cf. Albert (9), Theorem 23.

let $\pi = 2$. If $\mathfrak{D}$ is an algebra of the second kind then $\mathfrak{K} = \mathfrak{K}_0(q)$ where $q^T = q + 1$ contrary to Lemma 3. Thus $\mathfrak{D}$ must be of the first kind. We let $\mathfrak{K}_0 = \mathfrak{F}(A)$ and define α and V as in our proof of Lemma 3. Algebra $\mathfrak{D}$ over $\mathfrak{F}(A)$ is equivalent to a set of conjugate algebras $\mathfrak{D}_j$ over $\mathfrak{F}(\alpha_j)$ and

$$V\tau V' = \begin{pmatrix} R_1C_{11} & & \\ & \ddots & \\ & & R_tC_{tt} \end{pmatrix},$$

where R_j is a Weyl matrix over $\mathfrak{F}_j = \mathfrak{F}(\alpha_j)$ with $\mathfrak{D}_j$ over $\mathfrak{F}(\alpha_j)$ as a sub-algebra of its multiplication algebra $\mathfrak{A}_j$. If B is in $\mathfrak{D}$ then B^T is in $\mathfrak{D}$ and, since both B and B^T are commutative with A,

$$VBV^{-1} = \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_t \end{pmatrix}, \qquad VB^TV^{-1} = \begin{pmatrix} B_1^T & & \\ & \ddots & \\ & & B_t^T \end{pmatrix},$$

where $B_j^T = C_{jj}B_j'C_{jj}^{-1}$ is in $\mathfrak{D}_j$ for every B of $\mathfrak{D}$ and corresponding B_j of $\mathfrak{D}_j$. Then $\mathfrak{D}_j$ is a T-involutorial normal division algebra over $\mathfrak{F}_j$ and is a sub-algebra of $\mathfrak{A}_j$. By our above proof $\mathfrak{D}_j$ has degree unity over $\mathfrak{F}_j$. Hence $\mathfrak{D}$ has degree one over $\mathfrak{K}_0$ and $\mathfrak{D} = \mathfrak{K}_0$. We have proved the important

THEOREM 25. *Let R be an irreducible Weyl matrix over a field $\mathfrak{F}$ of characteristic not zero. Then the multiplication algebra of R is a T-symmetric field $\mathfrak{K}_0$.*

Theorem 25 evidently reduces our study of the multiplication algebra of a Weyl matrix R over $\mathfrak{F}$ to the case where $\mathfrak{F}$ is a non-modular field. In this case the centrum of $\mathfrak{A}$ is a field $\mathfrak{K}_0$ or $\mathfrak{K}_0(q)$, $q^T = -q$, and it becomes important to investigate the characteristic roots of matrices $A = \epsilon A^T$, $\epsilon = \pm 1$. We use our proof of Lemma 3 with $V\tau V^J = VRV^{-1}VCV^J$ and obtain

$$C_{jk}(\alpha_k - \epsilon\alpha_j^J) = 0\,, \tag{59.1}$$

so that

$$C_{jk} = 0 \qquad (\alpha_k \neq \epsilon\alpha_j^J)\,. \tag{60.1}$$

Then the regularity of $V\tau V^J$ of (61) implies that $\alpha_j = \epsilon\alpha_j^J$. We have proved

THEOREM 26. *Let $\epsilon = \pm 1$ and $A = \epsilon A^T$ be in the multiplication algebra $\mathfrak{D}$ of an irreducible Weyl matrix R over a non-modular field $\mathfrak{F}$. Then the characteristic roots of A satisfy*

$$\alpha_j = \epsilon\alpha_j^J\,. \tag{62}$$

4. **Definite Weyl matrices.** The matrices $\tau_1 = R_1 = 1$, $\tau_2 = R_2 = -1$ are both totally regular and non-isomorphic and yet $U\tau U'$ is not totally regular if

$$\tau = \begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \qquad U\tau U' = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}. \tag{63}$$

In our later treatment we shall find it desirable to *compose* Weyl matrices and hence shall restrict all further attention to the following case.[46]

Let $\Gamma \neq \Gamma_0$ be algebraically closed so that Γ_0 is real closed, $\Gamma = \Gamma_0(i)$, $i^2 = -1$. If $c = a + bi$ with a and b real (in Γ_0), then $\bar{c} = c^J = a - bi$ and $\tau^J = \bar{\tau}'$ may be called an Hermitian matrix. *We shall assume that every principal minor of τ has positive determinant.* Then *τ is positive definite and totally regular in* Γ and we call the corresponding Weyl matrices R *definite Weyl matrices.*

We may now prove a partial converse of Theorem 26.[47] Let R be any Weyl matrix with multiplication algebra $\mathfrak{A}$ and let A in $\mathfrak{A}$ have irreducible minimum equation and characteristic roots $\alpha_j = \epsilon\bar{\alpha}_j$, $\epsilon = \pm 1$. Then we have seen that

$$VRV^{-1} = \begin{pmatrix} R_1 & & \\ & \ddots & \\ & & R_t \end{pmatrix}, \qquad VC\bar{V}' = (C_{jk}), \tag{64}$$

so that $R_jC_{jj} = \tau_j$ is a principal minor of $V\tau\bar{V}'$ and is positive definite. Then so is

$$V\tau_0\bar{V}' = \begin{pmatrix} \tau_1 & & \\ & \ddots & \\ & & \tau_t \end{pmatrix}, \tag{65}$$

and $\tau_0 = RC_0$ where C_0 has elements in $\mathfrak{F}$ and it is well known[48] that C_0 may be chosen so that

$$VC_0\bar{V}' = \begin{pmatrix} C_{11} & & \\ & \ddots & \\ & & C_{tt} \end{pmatrix}. \tag{66}$$

Then $C_0\bar{A}'C_0^{-1} = \epsilon A = A^T$ and we have proved the converse

THEOREM 26C. *Let R be a definite Weyl matrix with multiplication algebra $\mathfrak{A}$ and $\tau = RC$ so that $\mathfrak{A}$ is T-involutorial with $A^T = C\bar{A}'C^{-1}$ for every A of $\mathfrak{A}$. Then if A in $\mathfrak{A}$ has irreducible minimum equation and characteristic roots $\alpha_j = \epsilon\,\bar{\alpha}_j$, $\epsilon = \pm 1$, there exists a positive definite matrix $\tau_0 = RC_0$ such that $A^{T_0} = C_0\bar{A}'C_0^{-1} = \epsilon\, A$ and $\bar{C}_0' = \delta\, C_0$ if $\bar{C}' = \delta C$.*

If R is any irreducible definite Weyl matrix of order p the matrix

$$R_0 = \begin{pmatrix} R & & & \\ & R & & \\ & & \ddots & \\ & & & R \end{pmatrix} \tag{67}$$

[46] An elaborate discussion of the total regularity of τ_0 would be necessary in the general case where τ is not assumed to be positive definite.

[47] Cf. Albert (1), p. 73, for the Riemann matrix case.

[48] Cf. Albert (2).

of order mp has multiplication algebra $\mathfrak{A} = \mathfrak{D} \times \mathfrak{M}$ where $\mathfrak{D}$ is the multiplication algebra of R and $\mathfrak{M}$ is a total matric algebra of degree m. The structure of $\mathfrak{D}$ is determined by that of $\mathfrak{A}$ and conversely. We may therefore use (67) to replace $\mathfrak{D}$ by a crossed product.

Let R be an irreducible definite Weyl matrix and $\mathfrak{K}$ be the centrum of $\mathfrak{D}$. Then $\mathfrak{K}$ is also the centrum of R_0 and we call R and R_0 *Weyl matrices of the first or second kinds* according as $\mathfrak{K}$ does not or does contain a T-skew quantity (where if A is in $\mathfrak{A}$ and $\tau = RC$ then

$$A^{T} = C\bar{A}'C^{-1}.) \tag{68}$$

If $\mathfrak{F} = \mathfrak{F}_0(q)$ then $q^T = -q$ and R is not of the first kind. Hence $\mathfrak{F}$ *is a real field* when R is of the first kind.

Suppose first that R is of the second kind. It is trivially shown that if $\mathfrak{D}$ has order $2n^2t$ over $\mathfrak{F}$, degree n over $\mathfrak{K}$, the number of linearly independent T-symmetric quantities of $\mathfrak{D}$ is n^2t over $\mathfrak{F}$, n^2 over $\mathfrak{K}$, and hence that $\mathfrak{D}$ has a basis of symmetric quantities with respect to $\mathfrak{K}$. Then obviously $\mathfrak{D}$ contains a maximal sub-field $\mathfrak{K}(x)$ with $x^T = x$. By Theorem 26 the root field of $\mathfrak{K}_0(x)$ is real and hence there exists a total real galois extension Z_0 of $\mathfrak{K}_0$ such that $Z = Z_0 \times \mathfrak{K}$ over $\mathfrak{K}$ is a splitting field for $\mathfrak{D}$. We have proved

THEOREM 27. *The multiplication algebra $\mathfrak{D}$ of any irreducible definite Weyl matrix R of the second kind is similar to a crossed product $\mathfrak{A} = \mathfrak{M} \times \mathfrak{D}$ of Theorem* 10, *where Z_0 is total real over $\mathfrak{K}_0$ and $\mathfrak{A}$ is the multiplication algebra of the definite Weyl matrix*

$$\begin{pmatrix} R & & \\ & \ddots & \\ & & R \end{pmatrix}. \tag{69}$$

We now let G, H range over all automorphisms of a total real galois extension Z_0 of $\mathfrak{K}_0$, $\mathfrak{A} = (Z, a)$ where $a = (a_{G,H})$, $a_{G,H} = a_{G,H1} \neq a_{G,H2}q$, $\mathfrak{K} = \mathfrak{K}_0(q)$ and $a_{G,H1}$ and $a_{G,H2}$ in Z_0. Write $\bar{a}_{G,H} = a_{G,H1} = a_{G,H2}q$ so that, by Theorem 10, there exist solutions d_G in Z_0 of

$$d_{GH}(d_G^H d_H)^{-1} = a_{G,H}\bar{a}_{G,H}\,. \tag{70}$$

We may prove

THEOREM 28. *Let $\mathfrak{A}$ be the multiplication algebra of a definite Weyl matrix of the second kind. Then* (70) *must have a set of total positive solutions d_G in Z_0.*

For τ is positive definite and so is $u_G\tau\bar{u}_G'$ where the u_G are a Z-basis of $\mathfrak{A}$. But by Theorem 26 algebra $\mathfrak{A}$ is T-involutorial with an involution T such that the quantities of Z_0 are T-symmetric. By our proof of Theorem 10 we must have $u_G^T = (u_Gd_G)^{-1}$ and hence

$$u_G^T = (u_Gd_G)^{-1} = (d_G^{G^{-1}}u_G)^{-1} = u_G^{-1}(d_G^{G^{-1}})^{-1} = C\bar{u}_S'C^{-1}\,. \tag{71}$$

Then $u_G\tau\bar{u}_G' = u_G R(C\bar{u}_S' C^{-1})C = u_G(u_G^T)\,\tau = (d_G^{G-1})^{-1}\tau$. Moreover if $Z_0 = \mathfrak{K}_0(y)$ we have

$$(72) \qquad VyV^{-1} = \begin{pmatrix} \alpha_1 I_r & & \\ & \ddots & \\ & & \alpha_t I_r \end{pmatrix}, \qquad V\tau\bar{V}' = \begin{pmatrix} \tau_1 & & \\ & \ddots & \\ & & \tau_r \end{pmatrix},$$

where $\tau_j = R_j C_j$ is positive definite. Hence so is

$$(73) \qquad Vf_G\tau V^{-1} = \begin{pmatrix} f_G(\alpha_1)\tau_1 & & \\ & \ddots & \\ & & f_G(\alpha_t)\tau_t \end{pmatrix},$$

where $f_G = (d_G^{S-1})^{-1}$ is in Z_0. But then $f_G\,(\alpha_j) > 0$ so that d_G must be total positive.

We next consider the case where $\mathfrak{D}$ is an algebra of the first kind and assume first that $\mathfrak{D}$ contains a symmetric quantity x of degree n over $\mathfrak{K} = \mathfrak{K}_0$ where n is the degree of $\mathfrak{D}$ over $\mathfrak{K}$. Then the *root field* of $\mathfrak{K}(x)$ is a total real galois extension of $\mathfrak{K}$ and $\mathfrak{D}$ is similar to a crossed product of Theorem 10. We also have immediately as in Theorem 28

THEOREM 29. *Let $\mathfrak{A} = (Z, a)$ over $\mathfrak{K} = \mathfrak{K}_0$ be defined by a total real galois field Z and be the multiplication algebra of a definite Weyl matrix R. Then the equations*

$$(74) \qquad d_{GH}(d_G^H d_H)^{-1} = (a_{G,H})^2$$

have a total positive set of solutions d_G in Z.

We next prove

THEOREM 30. *Let $\mathfrak{D}$ be the multiplication algebra of a Weyl matrix of the first kind and with no maximal T-symmetric sub-field. Then $\mathfrak{D}$ is similar to $\mathfrak{A} = \mathfrak{A}_1 \times Q$ where $\mathfrak{A}_1$ is a crossed product $\mathfrak{A}_1 = (Z_0, a)$, Z_0 total real, and*

$$(75) \qquad Q = (1, i, j, ij)\,, \qquad ji = -ij\,, \qquad i^2 = j^2 = -1\,.$$

Moreover $\mathfrak{A}$ contains no maximal T-symmetric sub-field and there exist a set of total positive solutions d_G of (74) in Z_0.

For let x be a T-symmetric quantity of $\mathfrak{D}$ of the largest possible grade with respect to $\mathfrak{K}$ and let $\mathfrak{B}$ be the algebra of all quantities of $\mathfrak{D}$ commutative with x. If $bx = xb$ then $b^T x = xb^T$ and $\alpha = b + b^T$, $\beta = bb^T$ are symmetric and hence in $\mathfrak{K}(x)$. Then b is a root of $x^2 - \alpha x + \beta = (x - b)\,(x - b^T) = 0$ and β has degree one or two over $\mathfrak{K}(x)$, $\mathfrak{K}(x)$ has degree n or $n/2$ over $\mathfrak{K}$ where n is the degree of $\mathfrak{D}$ over $\mathfrak{K}$. We have considered the former case and hence restrict our attention to the case where

$$(76) \qquad \mathfrak{B} = (1, v, w, vw)\,, \qquad vu = -uv\,, \qquad v^2 = -\alpha\,, \qquad w^2 = -\beta$$

with α and β in $\mathfrak{K}(x)$.

The only symmetric quantities of $\mathfrak{B}$ are the quantities of $\mathfrak{R}(x)$ and hence we may take $v^T = -v$, $w^T = -w$ so that α and β must be total positive quantities of $X = \mathfrak{R}(x)$. If X_0 is a scalar field isomorphic to X and α_0, β_0 of X_0, correspond to α, β of X then $X_0(\alpha_0^{1/2}, \beta_0^{1/2})$ is total real. The corresponding root field Z_0 is a total real galois field which does not split $\mathfrak{D}$ but $\mathfrak{D}_{Z_0}$ is the direct product of a total matric algebra and Q of (75). If $Z = (Z_0, i_0)$ where $i_0^2 = -1$ then Z splits $\mathfrak{D}$ and if $\mathfrak{A}$ is the crossed product defined by Z and similar to $\mathfrak{D}$ then the sub-algebra of all quantities of $\mathfrak{A}$ commutative with every quantity of Z_0 is equivalent to $\mathfrak{B}$ over Z_0. But evidently $\mathfrak{B}_{Z_0} = Q \times Z_0$ and hence $\mathfrak{A} = \mathfrak{A}_1 \times Q$ where $\mathfrak{A}_1 = (Z_0, a)$. Moreover if P is the field of all real numbers than $\mathfrak{A}_P \sim Q$ is not a total matric algebra and $\mathfrak{A}$ can have no maximal symmetric sub-field.

We now let $\mathfrak{A} = \mathfrak{A}_1 \times Q$ be the multiplication algebra of R_0. If L is the automorphism of $Z = Z_0 \times \mathfrak{R}(i)$ which replaces i by $-i$ we may take $j = u_L$ and L commutative with all the automorphisms of Z, u_L commutative with all the u_G. By Theorem 15 we may take

$$i^T = -i\,, \qquad z_0^T = z_0\,, \tag{77}$$

for every z of Z_0. The algebra $\mathfrak{A}_1$ has exponent at most two and hence (76) has solutions d_G in Z_0. Then we will complete the proof of Theorem 30 if we can prove that $u_G^T = (u_G d_G)^{-1}$ with d_G in Z_0 and G ranging over all automorphisms of Z_0.

Algebra $\mathfrak{A}$ is J-involutorial with $i^J = -i$, $j^J = -j$, $z_0^J = z_0$, $u_G^J = (u_G c_G)^{-1}$ with c_G in Z_0 and a solution of (74). By Corollary I to Theorem 4 we have

$$A^T = p^{-1}a^J p\,, \tag{78}$$

where p is in $Z = Z_0(i)$ and $p^T = \pm p$. If $p^T = -p$ then $p = p_0 i$ with p_0 in Z_0 and $j^T = i^{-1}p_0^{-1}(-j)p_0 i = j$ contrary to hypothesis. Hence p is in Z_0 and $\mathfrak{A}_1$ is itself T-involutorial. Then $u_G^T = (u_G d_G)^{-1}$ with d_G in Z_0 and, as in the proof of Theorem 28, d_G must be total positive.

The conditions of Theorems 28, 29, 30 are sufficient as well as necessary that $\mathfrak{D}$ shall be the multiplication algebra of an R. We shall give the existence theorems in our last chapter.

IV. Central Weyl Matrices

1. **The $\mathfrak{F}$-algebra of a Weyl matrix.** Let R be a Weyl matrix defined by $\tau = RC$ and let $\mathfrak{B}$ be the set of all square matrices A with elements in $\mathfrak{F}$ such that $R^{-1}AR = B$ has elements in $\mathfrak{F}$. Then $\mathfrak{B}$ is a linear associative algebra over $\mathfrak{F}$ and we call $\mathfrak{B}$ the $\mathfrak{F}$-algebra of R. Evidently $AR = RB$ if and only if $GAG^{-1}(GRH) = (GRH)\,H^{-1}BH$. Thus *associated Weyl matrices have equivalent $\mathfrak{F}$-algebras.* When $G = I_p$ then R has the same $\mathfrak{F}$-algebra as RH. In particular R and τ have the same $\mathfrak{F}$-algebras.

2. Central Weyl matrices. The $\mathfrak{F}$-algebra $\mathfrak{B}$ of a Weyl matrix R contains its multiplication algebra $\mathfrak{A}$. We call R a *central Weyl matrix* if $\mathfrak{B} = \mathfrak{A}$. Then R is central when $AR = RB$ if and only if $A = B$, $AR = RA$.

Let $\mathfrak{F} = \mathfrak{F}_0$ and $\tau = \tau_1 + \tau_2\rho$ where $\tau_1 = \tau_1' \neq 0$ and $\tau_2 = -\tau_2' \neq 0$. Then we shall assume that either τ_1 or τ_2 is non-singular. If $\mathfrak{F} \neq \mathfrak{F}_0$ or one of τ_1 and τ_2 is zero then the non-singularity of τ will be sufficient and we make no further restriction. With this hypothesis[49] we prove

THEOREM 31. *Every Weyl matrix R satisfying the above restriction is associated with a central Weyl matrix R_0 defined by the same $\tau = RC = R_0C_0$. Moreover if $\tau = \tau'$, $\mathfrak{F} = \mathfrak{F}_0$, then we may take $C_0 = C_0'$.*

For the matrices τ_1, τ_2 have only a finite number of elements and hence

$$(79) \qquad \tau = \sum_{i=1}^{e} \xi_i (C_i + D_i \rho), \qquad C_i' = C_i, \qquad D_i' = -D_i,$$

where C_i and D_i have elements in $\mathfrak{F}_0$, $\xi_1, \cdots, \xi_e$ are in Γ_0 and linearly independent in $\mathfrak{F}_0$. If $\mathfrak{F} = \mathfrak{F}_0$ then $\xi_1, \cdots, \xi_e, \xi_1\rho, \cdots, \xi_e\rho$ are linearly independent in $\mathfrak{F}$. But then $A\tau - \tau B = \sum_i \xi_i [A(C_i + D_i\rho) - (C_i + D_i\rho)B] = 0$ so that $A C_i = C_iB$, $AD_i = D_iB$. Then $A(\Sigma\eta_i \cdot C_i + \zeta_iD_i) = (\Sigma\eta_iC_i + \zeta_iD_i)B$ identically η_i, ζ_i. If τ_1 is non-singular the determinant of $\Sigma\eta_iC_i$ is not zero for $\eta_i = \xi_i$ and hence does not vanish identically in the η_i. Then there exist η_{i0} in $\mathfrak{F}$ such that $C_0 = \Sigma\eta_{i0}C_i = C_0'$ is non-singular and $AC_0 = C_0B$. If τ_2 is non-singular then $C_0 = \Sigma\zeta_{i0}D_i$ is non-singular for ζ_{i0} in $\mathfrak{F}$ and $C_0' = -C_0$, $AC_0 = C_0B$. In either case $R_0 = \tau C_0^{-1}$ is a central Weyl matrix since if $AR_0 = R_0A$ then $A\tau C_0^{-1} = \tau C_0^{-1} A_0$, $A\tau = \tau B$ where $B = C_0^{-1} AC_0 = C_0^{-1}A_0C_0$, $A = A_0$.

Let next $\mathfrak{F} \neq \mathfrak{F}_0$ so that $\tau = \tau^J$ is non-singular and we may write $\tau = \sum_{i=1}^{e} \xi_iH_i$ where $\xi_1, \cdots, \xi_e$ are in Γ_0 and are linearly independent in $\mathfrak{F}$,

$$H_i = C_i \neq D_i\rho = H_i^J$$

has elements in $\mathfrak{F}$. Then $A\tau = \tau B$ implies that $AH_i = H_iB$ and hence there exists a non-singular matrix $C_0 = \Sigma\xi_{i0}H_i = C_0^J$ such that $AC_0 = C_0B$. Thus $R_0 = \tau C_0^{-1}$ is a central Weyl matrix.

We next prove

THEOREM 32. *Let $R_1 = U^{-1}R_0 U$ be isomorphic to a central Weyl matrix R_0. Then R_1 is a central Weyl matrix.*

For if $A_1R_1 = R_1B_1$ then $A_1U^{-1}R_0U = U^{-1}R_0UB_1$, $(UA_1U^{-1})R_0 = R_0UB_1U^{-1}$. Since R_0 is central, $UA_1U^{-1} = UB_1U^{-1}$ and $A_1 = B_1$.

3. A generalized Schur Lemma. The *Schur Lemma* does not suffice for our

[49] We shall later study the question of the existence of $C = \epsilon C'$ such that $CA^JC^{-1} = A^T$ for A in a given algebra $\mathfrak{A}$. These later results will enable us to prove Theorem 31, as a corollary of Theorem 55, without the above hypothesis.

later work where we study associated Weyl matrices so we shall prove the generalization.

THEOREM 33. *Let the $\mathfrak{F}$-algebra of either of two p-rowed Weyl matrices R and S be a division algebra and let*

$$BR = SA\,, \tag{80}$$

for p-rowed square matrices A and B with elements in $\mathfrak{F}$. Then either AB is non-singular and S is associated with R, or $A = B = 0$.

We first prove the

LEMMA. *Let τ be a positive definite Hermitian matrix. Then $\bar{A}'\,\tau\,A = 0$ if and only if $A = 0$.*

For there exist non-singular matrices P and Q such that

$$PAQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \tag{81}$$

where r is the rank of A. If $r > 0$ then

$$0 = (\overline{PAQ})'\,(\bar{P}^{-1})'\,\tau\,P^{-1}(PAQ) = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \tau_1 & \tau_2 \\ \tau_3 & \tau_4 \end{pmatrix}\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \tau_1 & 0 \\ 0 & 0 \end{pmatrix},$$

so that $\tau_1 = 0$. But $(\bar{P}^{-1})'\,\tau\,P^{-1}$ is positive definite and cannot have a zero principal minor τ_1 of order r. This gives the lemma.

Now let $\tau = RC$, $\sigma = SC$, and assume without loss of generality that the $\mathfrak{F}$-algebra of R is a division algebra. Then $B\,\tau = \sigma\,A_0$ where $A_0 = C_1^{-1}AC$ and hence $\tau\bar{B}' = \bar{A}'_\sigma\sigma$,

$$\bar{A}'_0\,\sigma\,A_0 = \tau(\bar{B}'A_0) = (\bar{A}'_0B)\tau\,. \tag{82}$$

Hence $\bar{B}'A_0$ is in the $\mathfrak{F}$-algebra of τ and $\bar{B}'A_0$ *is non-singular or is zero.* In the former case AB is non-singular as desired. In the latter case $\bar{A}'_0\,\sigma\,A_0$ is zero which is impossible unless A_0 is zero by our lemma. Hence $A = 0$ and, since R is non-singular and $BR = S$. $= 0$, $B = 0$.

4. **Reduction theory.** We may prove

THEOREM 34. *Every reducible central Weyl matrix is isomorphic to*

$$R_0 = \begin{pmatrix} S_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & S_t \end{pmatrix}, \quad S_i = \begin{pmatrix} R_i & & & \\ & \cdot & & \\ & & \cdot & \\ & & & R_i \end{pmatrix} \tag{83}$$

where the R_i are irreducible central Weyl matrices such that R_i and R_j are not associated for $i \neq j$. Conversely every R_0 of the above form is a central Weyl matrix.

For by our reduction theory for Weyl matrices and by Theorem 32 we may take R_0 in the form (83) with the R_i as irreducible components and R_i not

isomorphic to R_j for $i \neq j$. If $A_iR_i = R_iB_i$ then

$$\begin{bmatrix} 0 & & & & \\ & \cdot & & & \\ & & A_i & & \\ & & & \cdot & \\ & & & & 0 \end{bmatrix} \begin{bmatrix} R_1 & & & & \\ & \cdot & & & \\ & & R_i & & \\ & & & \cdot & \\ & & & & \cdot \end{bmatrix} = \begin{bmatrix} R_1 & & & & \\ & \cdot & & & \\ & & R_i & & \\ & & & \cdot & \\ & & & & \cdot \end{bmatrix} \begin{bmatrix} 0 & & & & \\ & \cdot & & & \\ & & B_i & & \\ & & & \cdot & \\ & & & & 0 \end{bmatrix},$$

and the property that R_0 is a central Weyl matrix implies that $A_i = B_i$, the R_i are central. If $GR_k = R_sH$ for G and H non-singular matrices and $G \neq H$ then $A_{sk}S_k = S_sB_{sk}$ where A_{sk} is a matrix of diagonal blocks G and other blocks of zeros, B_{sk} is a matrix of diagonal blocks H and other blocks of zeros. But we put $A = (A_{ij}) \neq B = (B_{ij})$ with $A_{ij} = B_{ij} = 0$ unless $i = s$, $j = k$ and have $AR_0 = R_0B$ contrary to hypothesis. Hence R_i is not associated with R_j for $i \neq j$.

Conversely let R_0 have the from (83). If $AS_i = S_mB$ then $A_{jk}R_i = R_mB_{jk}$. By Theorem 33 $A_{jk} = B_{jk} = 0$ for $i \neq m$. If $i = m$ then $A_{jk}R_i = R_iB_{jk}$ implies that $A_{jk} = B_{jk}$ and $A = B$. Hence S_i is a central Weyl matrix and $AS_i = S_mB$ implies that $A = B = 0$ for $i \neq m$. Suppose then that $AR_0 = R_0B$, $A_{ij}S_j = S_iB_{ij}$. If $i \neq j$ then $A_{ij} = B_{ij} = 0$. If $i = j$ then $A_{ij} = B_{ij}$ so that $A = B$ and we have proved Theorem 34.

5. **The Weyl matrices associated with a central definite Weyl matrix.** Let R be a central Weyl matrix and let R_0 be associated with R. Then $R_0 = HRG$ where G and H are non-singular and R_0 is isomorphic to $H^{-1}R_0H = RGH$. Hence we may assume

$$R_0 = RG \tag{84}$$

without loss of generality. We shall prove

THEOREM 35. *Let C_0 be a principal matrix of R_0. Then*

$$G = CC_0^{-1}, \qquad \tau = RC = R_0C_0, \tag{85}$$

where C is a principal matrix of R.

For if $\tau_0 = R_0C_0$ and $\tau = RC$ are positive definite Hermitian matrices then $\tau_0 = RGC_0 = \tau C^{-1}GC_0$, $\bar{C}_0' = \epsilon_0C$, $\bar{C}' = \epsilon C$, $\epsilon_0 = \pm 1$, $\epsilon = \pm 1$. We obtain $\bar{\tau}_0' = \overline{(C^{-1}GC_0)}'\,\tau = \tau_0 = RGC_0 = \overline{(GC_0)}'\,\epsilon\, C^{-1}RC$ and hence $RGC_0C^{-1} = \epsilon\,\overline{(GC_0)}'C^{-1}R$. But R is a central Weyl matrix so that $GC_0 = \epsilon\overline{(GC_0)}' = C_1$, $RC_1 = \tau_0$ is positive definite and C_1 is a principal matrix of R. Then $G = C_1C_0^{-1}$ as desired.

Theorem 35 evidently implies that the most general Weyl matrix associated with R is the isomorphic to a matrix of the form

$$RCC_0^{-1}, \tag{86}$$

where C is a principal matrix of R and $C_0 = \pm \bar{C}_0'$ is any non-singular matrix with elements in $\mathfrak{F}$. Since C_0 is absolutely arbitrary apart from its property $C_0 = \pm C_0^J$ the following theorem completes the theory of this section.

THEOREM 36. *Let R be a central definite Weyl matrix over $\mathfrak{F}$ with principal matrix C and multiplication algebra $\mathfrak{A}$ and let*

$$R_0 = RG , \qquad G = CC_0^{-1} \tag{87}$$

where $C_0 = \epsilon_0 C_0^J$, $\epsilon_0 = \pm 1$. Then R_0 is a Weyl matrix associated with R and the multiplication algebra of R_0 is the algebra $\mathfrak{B}$ of all quantities of $\mathfrak{A}$ commutative with G.

For if $AG = GA$, $AR = RA$ then $ARG = RGA$ and A is in $\mathfrak{A}$. Conversely let $AR_0 = R_0A = ARG = RGA$ so that $AR = RGAG^{-1}$. Since R is a central Weyl matrix $A = GAG^{-1}$ is in $\mathfrak{A}$. Obviously $\tau = RC = R_0G^{-1}C = R_0C_0C^{-1}C = R_0C_0$ so that R_0 is a Weyl matrix associated with R.

6. **The Weyl matrix R^{-1}.** Let R be a central Weyl matrix and $\tau = RC$, $C^J = \pm C$, $R^J = \pm C^{-1}RC$. Then $R^{-1}(\pm C) = C\tau^{-1}C^J$ is positive definite so that R^{-1} is a Weyl matrix over $\mathfrak{F}$ with $\pm C$ as principal matrix. If $AR^{-1} = R^{-1}B$ then $RA = BR$ so that $B = A$ is in the multiplication algebra of R. Conversely $AR = RA$ implies that $R^{-1}A = AR^{-1}$ and A is in the multiplication algebra of R^{-1}. We have proved

THEOREM 37. *Let R be a central Weyl matrix over $\mathfrak{F}$ with principal matrix $C = \epsilon \bar{C}'$, $\epsilon = \pm 1$. Then R^{-1} is a central Weyl matrix over $\mathfrak{F}$ with principal matrix ϵC and the same multiplication algebra as R.*

Assume now that R is irreducible and has multiplication algebra $\mathfrak{D}$ over $\mathfrak{F}$. Then R^{-1} is also irreducible and $\mathfrak{D}$ is its multiplication algebra. We let

$$GR^{-1} = RH , \qquad G \neq 0, \tag{88}$$

where G and H have elements in $\mathfrak{F}$. By Theorem 33 the matrices G and H are non-singular.

Suppose also that $G_1R^{-1} = RH_1$ whence $G_1G^{-1}R = RH_1H^{-1}$ and $G_1 = XG$, $H_1 = XH$ where X is in $\mathfrak{D}$. In particular $(GR^{-1})^{-1} = RG^{-1} = H^{-1}R^{-1}$ so that

$$HG = GH = -Y \text{ in } \mathfrak{D} . \tag{89}$$

Let A be in $\mathfrak{D}$. Then $AR^{-1} = R^{-1}A$ and $AG^{-1}RH = G^{-1}RHA$, $(GAG^{-1})R = RHAH^{-1}$. Thus

$$GAG^{-1} = A_0 = HAH^{-1} \tag{90}$$

is in $\mathfrak{D}$ for every A of $\mathfrak{D}$.

Equation (88) implies that $RHR = \tau C^{-1}H \, \tau C^{-1} = G$, $\tau A \tau = B$ where

$$A = C^{-1}H , \quad B = GC .$$

But $\tau A \tau = B$ implies that $\tau A^J \tau = B^J$ and thus $A^J = C^{-1}H_1$, $B^J = G_1C$. We obtain $\epsilon CG^J = G_1C$, $G_1 = \epsilon CG^JC^{-1}$, while similarly $H_1 = \epsilon CH^JC^{-1}$,

$$CG^JC^{-1} = \beta G , \quad CH^JC^{-1} = \beta H , \quad \beta \text{ in } \mathfrak{D} . \tag{91}$$

Consider the algebra $\mathfrak{D}_0$ of all matrices

$$a_A = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}, \tag{92}$$

where A ranges over all quantities of $\mathfrak{D}$. Then $\mathfrak{D}_0$ is evidently equivalent to $\mathfrak{D}$ under the correspondence in which a_A corresponds to A. Let also $\mathfrak{A} = \mathfrak{D}_0 + \mathfrak{D}_0 G$ where

$$g = \begin{pmatrix} 0 & H \\ -G & 0 \end{pmatrix}. \tag{93}$$

Then $A_0 = GAG^{-1}$,

$$g^2 = \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix}, \qquad g a_A g^{-1} = a_{A_0}, \tag{94}$$

are in $\mathfrak{D}_0$ for every A of $\mathfrak{D}$. Hence $\mathfrak{A}$ is an algebra over $\mathfrak{F}$ with $\mathfrak{D}_0$ as sub-algebra. If

$$E = \begin{pmatrix} I_p & 0 \\ 0 & -I_p \end{pmatrix},$$

then $Ea_AE^{-1} = a_A$, $EgE^{-1} = -g$ so that all quantities of the linear set $\mathfrak{D}_0$ are commutative with E, all of $\mathfrak{D}_0 g$ are transformed into their negatives by E. We have proved

THEOREM 38. *Let R be an irreducible central Weyl matrix with multiplication algebra $\mathfrak{D}$ and*

$$G = RHR \qquad (G \neq 0), \tag{95}$$

for G and H with elements in $\mathfrak{F}$. Then $GH = HG = Y$ in $\mathfrak{D}$, the algebra $\mathfrak{D}_0$ of matrices a_A in (92) *is equivalent to $\mathfrak{D}$, and the linear set $\mathfrak{A} = \mathfrak{D}_0 + \mathfrak{D}_0 g$ given by* (93), (94) *is an algebra over $\mathfrak{F}$.*

Algebra $\mathfrak{D}$ is a T-involutorial algebra with $A^T = CA^JC^{-1}$. Write

$$C_0 = \begin{pmatrix} 0 & C \\ -C & 0 \end{pmatrix}, \qquad C_0^J = -\epsilon C_0, \tag{96}$$

and hence

$$C_0 a_A^J C_0^{-1} = \begin{pmatrix} A_T^J & 0 \\ 0 & A^J \end{pmatrix} = a_{A^T}. \tag{97}$$

Then $\mathfrak{D}_0$ is also T-involutorial with $(a_A)^T = a_{A^T}$. We also compute

$$C_0 g^J C_0^{-1} = \begin{pmatrix} 0 & CH^JC^{-1} \\ -CG^JC^{-1} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \beta H \\ -\beta G & 0 \end{pmatrix} = a_\beta g \equiv g^T, \tag{98}$$

and $\mathfrak{A}$ is T-involutorial with sub-algebra $\mathfrak{D}_0$ closed under T.

Consider first the case where g is commutative with all the quantities of the centrum $\mathfrak{K}^0$ of $\mathfrak{D}_0$. Then $\mathfrak{A}$ over $\mathfrak{K}^0$ contains a normal division algebra $\mathfrak{D}_0$ over $\mathfrak{K}^0$ and $\mathfrak{A}$ is the direct product of $\mathfrak{D}_0$ and an algebra $\mathfrak{G}$ of order two over $\mathfrak{K}^0$. But $\mathfrak{G} = (1, h)$, $h^2 = a_\delta$ in $\mathfrak{K}^0$, $h = a_1 + a_2 g$ with a_1 and $a_2 \neq 0$ in $\mathfrak{D}_0$. Without loss of generality we may replace G by $G_1 = a_2 G$ and hence may take $h = a_1 + g$. Then $ah = aa_1 + ag = ha = a_1 a + a_0 g$ for every a of $\mathfrak{D}_0$. The quantities 1, g are left linearly independent in $\mathfrak{D}_0$, $a = a_0$ and $a_1 a = aa_1$. Hence a_1 is in $\mathfrak{K}^0$, $h^2 = a_1^2 + q^2 + 2a_1 q$ is in $\mathfrak{K}^0$ so that $a_1 = 0$, $h = g$, $q^2 = a_\delta \neq 0$ in $\mathfrak{K}^0$.

Every a of $\mathfrak{D}_0$ defines an a^T in $\mathfrak{D}_0$ and $(a^T)^T = a$. Since $ga^T = a^T g$ we have $g^T a = ag^T$, $g^T = a_\beta g$ so that $a_\beta a = aa_\beta$ for every a of $\mathfrak{D}_0$. Thus a_β is in $\mathfrak{K}^0$ and either $a_\beta = -1$, $g^T = -g$ or $g + g^T = (a_\beta + 1)\, g \neq 0$ is T-symmetric and may be taken to replace g. Hence $g^T = \pm\, g$, $g^2 = a_\delta$, $\delta = \delta^T$, and by (89), (94), (95) we have

$$R_0 = RH\,, \qquad R_0^2 = -\delta \text{ in } \mathfrak{K}\,. \tag{99}$$

But we have shown that we may take $\beta = \pm 1$ in (91), $CH^J C^{-1} = \beta H$, $(H^{-1}C)^J = C^J(H^J)^{-1} = \beta\epsilon(H^{-1}C)$. Put $\epsilon_0 = \beta\epsilon$ and Theorem 36 states that RH is a Weyl matrix over $\mathfrak{F}$ with $C_0 = H^{-1}C$ as principal matrix. Moreover $HAH^{-1} = A$ for every A of $\mathfrak{D}$ by (90) and our above proof so that we have

THEOREM 39. *Let the matrix G of* (95) *be commutative with all quantities of the centrum $\mathfrak{K}$ of $\mathfrak{D}$. Then G may be so chosen that the matrix $R_0 = RH$ is a central Weyl matrix with multiplication algebra $\mathfrak{D}$ and principal matrix $C_0 = \epsilon_0 C_0^J$ and such that there exists a quantity $\delta = \delta^T$ in the centrum of $\mathfrak{D}$ for which*

$$R_0^2 = -\delta. \tag{100}$$

Moreover $-\delta R_0^{-1} = R_0$, $\mathfrak{A}_0 = \mathfrak{D}_0 + \mathfrak{D}_0 g_0$ is equivalent to $\mathfrak{A}$ where

$$g_0 = \begin{pmatrix} 0 & I_p \\ \delta & 0 \end{pmatrix}. \tag{101}$$

If $\delta = \lambda^{-2}$ with λ in $\mathfrak{K}$ we replace g by $a_\lambda \cdot g$ and have $\delta = 1$, $\mathfrak{A} = \mathfrak{D}_1 \oplus \mathfrak{D}_2$ where the $\mathfrak{D}_i$ are equivalent to $\mathfrak{D}$. If δ is not the square of any quantity λ in $\mathfrak{K}$ the algebra $(1, q)$ over $\mathfrak{K}^0$ is a *commutative division algebra of order two over* $\mathfrak{K}^0$ (quadratic field) and it is well known[50] that either $\mathfrak{A}$ is a division algebra over $\mathfrak{K}^0(q)$ or $\mathfrak{A} = \mathfrak{M}_2 \times \mathfrak{B}$ where $\mathfrak{B}$ is a normal division algebra over $\mathfrak{K}_0(q)$ and $\mathfrak{M}_2$ is a total matric algebra of degree two. We have

THEOREM 40. *If the algebra $\mathfrak{A}$ of Theorem* 39 *is not a division algebra then either we may take $R_0^2 = -1$ and $\mathfrak{A} = \mathfrak{D}_1 \oplus \mathfrak{D}_2$, $\mathfrak{D}_i \cong \mathfrak{D}$, or $\mathfrak{A} = \mathfrak{M}_2 \times \mathfrak{B}$ where $\mathfrak{B}$ is a division algebra and $\mathfrak{M}_2$ is a total matric algebra of degree two.*

We now assume that g is not commutative with all quantities in the centrum $\mathfrak{K}^0$ of $\mathfrak{D}_0$. If k is in $\mathfrak{K}^0$ then so is $k_0 = gkg^{-1}$. Hence $\mathfrak{K}^0$ is an involutorial[51] field and Theorem 2 states that there exists a sub-field Σ of $\mathfrak{K}^0$ such that $\mathfrak{K}^0 = \Sigma(u)$,

[50] Albert (10).

[51] For g^2 is in $\mathfrak{D}_0$ and hence $gk_0 g^{-1} = k_{00} = k$ for every k of $\mathfrak{K}$.

$gu = -ug$, $k_0 = k$ for every k_0 of Σ, $u^2 = \alpha$ in Σ. We may take $g^T = \pm g$ as before and have $gu = -ug$, $u^T g = -gu^T$. Hence $g(u \pm u^T) = -(u \pm u^T)g$ so that we may take $u^T = \phi u$, $\phi = \pm 1$. The centrum of $\mathfrak{A}$ is obviously Σ and it is well known[50] that $\mathfrak{A}$ is a normal simple algebra over Σ. But $\mathfrak{D}_0$ is a division algebra so that either $\mathfrak{A}$ is a division algebra or $\mathfrak{A} = \mathfrak{M}_2 \times \mathfrak{B}$ where $\mathfrak{M}_2$ is a total matric algebra of degree two and $\mathfrak{B}$ is a normal division algebra over Σ. Write $H = -YG^{-1}$ and (88), (89), (90) give the equivalent conditions

$$(102) \qquad Y = Y^T \text{ in } \mathfrak{D}, \qquad YRG^{-1}R = G, \qquad YG = GY,$$

$$(103) \qquad (Y^{-1}G^2)A = A(Y^{-1}G^2),$$

for every A of $\mathfrak{D}$. We also have

$$(104) \qquad UR = RU, \qquad GU = -UG, \qquad \mathfrak{R} = \Sigma(U)$$

where Σ is the centrum of $\mathfrak{A}$, $\mathfrak{R}$ is the centrum of $\mathfrak{D}$. We shall use the above conditions later. We have proved

THEOREM 41. *Let the condition on G of Theorem 39 be not satisfied so that (102)–(104) hold. Then $\mathfrak{A}$ is a normal simple algebra over Σ and is a division algebra or $\mathfrak{A} = \mathfrak{B} \times \mathfrak{M}_2$, $\mathfrak{B}$ a division algebra, $\mathfrak{M}_2$ a total matric algebra of degree two.*

V. OMEGA MATRICES[52]

1. The matrices Ω and R_Ω. Let C have elements in $\mathfrak{F}$ and the property that $C_0 = i_0 C$ is a Hermitian matrix for either $i_0 = 1$ or $i_0 = i$. Consider a p-rowed square matrix

$$(105) \qquad \Omega = \begin{pmatrix} \omega_1 \\ \bar{\omega}_2 \end{pmatrix},$$

with elements in Γ, such that ω_1 has r rows and

$$(106) \qquad w_1 C\omega_2' = 0; \qquad \gamma_1 = \omega_1 C_0 \bar{\omega}_1', \qquad \gamma_2 = -\bar{\omega}_2 C_0 \omega_2'$$

are positive definite Hermitian matrices. Then

$$(107) \qquad \Phi = \Omega C_0 \bar{\Omega}' = \begin{pmatrix} \gamma_1 & 0 \\ 0 & -\gamma_2 \end{pmatrix},$$

so that Ω and C_0 are non-singular and r is *the index of the Hermitian matrix* C_0. We call Ω *an Omega matrix of order p over $\mathfrak{F}$ with C as principal matrix.* The unit i_0 and the index r of Ω are uniquely determined by C.

Define

$$(108) \qquad E_r = \begin{pmatrix} I_r & 0 \\ 0 & -I_{p-r} \end{pmatrix},$$

so that $E_r\Phi$ is positive definite Hermitian. Then if

$$(109) \qquad R_\Omega = i_0^{-1}\Omega^{-1}E_r\Omega,$$

[52] Cf. Albert (1).

the matrix $R_\Omega C = \Omega^{-1}E_r\Omega C = \Omega^{-1}E_r\Phi(\bar{\Omega}^{-1})'$ is positive definite Hermitian so that R_Ω is a Weyl matrix over $\mathfrak{F}$ with C as principal matrix and the property

$$(R_\Omega)^2 = i_0^{-2}I_p = \pm I_p. \tag{110}$$

Conversely let R be a Weyl matrix with principal matrix C and such that $R^2 = \epsilon_1 I_p$, $\epsilon_1 = \pm 1$. Let

$$i_0^2 = \epsilon_1, \qquad C_0 = i_0 C, \qquad R_0 = i_1^{-1}R,$$

so that $R_0^2 = I_p$, $RC = R_0C_0 = \tau$ is positive definite Hermitian. Then R_0 is a square root of the identity matrix I_p and it is known[53] that there exists a non-singular square matrix Ω with elements in $\mathfrak{F}$ such that $R_0 = \Omega^{-1}E_r\Omega$.
Let $\bar{C}_0' = \epsilon_0 C_0$, $\epsilon_0 = \pm 1$.

The matrix $\tau = R_0C_0$ is positive definite and hence so is

$$\tau_0 = \Omega\tau\bar{\Omega}' = E_r\Omega C_0\bar{\Omega}' = \bar{\tau}_0' = \epsilon_0\Omega C_0\bar{\Omega}'E_r. \tag{111}$$

Then

$$\Omega C_0\bar{\Omega}' = \begin{pmatrix}\gamma_1 & \gamma_3\\ \gamma_4 & -\gamma_2\end{pmatrix}, \qquad \tau_0 = \begin{pmatrix}\gamma_1 & \gamma_3\\ -\gamma_4 & \gamma_2\end{pmatrix} = \begin{pmatrix}\epsilon_0\gamma_1 & -\epsilon_0\gamma_3\\ \epsilon_0\gamma_4 & \epsilon_0\gamma_2\end{pmatrix}. \tag{112}$$

If $\epsilon_0 = -1$ then the complementary principal minors γ_1 and γ_2 of the positive definite Hermitian matrix τ_0 are zero, which is impossible. Hence $\epsilon_0 = 1$, $\gamma_3 = \gamma_4 = 0$. Thus *C_0 is Hermitian, i_0 is our previously defined integer*, and we have proved

THEOREM 42. *Let $C = \pm\bar{C}'$, $C_0 = i_0C = \bar{C}_0'$ be a Hermitian matrix of index r. Then a p-rowed square matrix R is a Weyl matrix over $\mathfrak{F}$ with principal matrix C and $R^2 = \pm I_p$ if and only if*

$$R = R_\Omega = i_0^{-1}\Omega^{-1}E_r\Omega, \tag{113}$$

where Ω is an Omega matrix of index r over $\mathfrak{F}$ with C as principal matrix. Hence $R^2 = \epsilon I_p$ implies that $C = \epsilon\bar{C}'$.

An Omega matrix

$$\Omega_0 = \begin{pmatrix}\omega_{01}\\ \bar{\omega}_{02}\end{pmatrix}$$

of the same order and index as Ω is said to be isomorphic to Ω if there exists a non-singular matrix A with elements in $\mathfrak{F}$ such that

$$\alpha_1\omega_1 = \omega_{01}A, \qquad \alpha_2\bar{\omega}_2 = \bar{\omega}_{02}A \tag{114}$$

for matrices α_1, α_2. Obviously (114) is equivalent to

$$\Omega_0 A\Omega^{-1} = \begin{pmatrix}\alpha_1 & 0\\ 0 & \alpha_2\end{pmatrix}, \tag{115}$$

---

[53] Wedderburn (4), section 8.04.

and hence Ω and Ω_0 are isomorphic if and only if $\Omega_0 A \Omega^{-1}$ is commutative with E_r for some non-singular A with elements in $\mathfrak{F}$. We note that if C is a principal matrix of Ω then $C^{(0)} = AC\bar{A}'$ is a principal matrix of Ω_0.

If $\Omega_0 A \Omega^{-1}$ is commutative with E_r then R_Ω and R_{Ω_0} have the same order and index and we have $\Omega_0 A \Omega^{-1} E_r = E_r \Omega_0 A \Omega^{-1}$ $i_0 A \Omega^{-1} E_r \Omega = i_0 \Omega_0^{-1} E_r \Omega_0 A$, $AR_\Omega = R_{\Omega_0} A$. Then R_Ω and R_{Ω_0} are isomorphic. Conversely if R_Ω and R_{Ω_0} are isomorphic they obviously have the same order, the same i_0, and the same index, and $AR_\Omega = R_{\Omega_0} A$ implies that Ω and Ω_0 are isomorphic. We have proved

THEOREM 43. *Two Weyl matrices R_Ω and R_{Ω_0} are isomorphic if and only if the corresponding Omega matrices Ω and Ω_0 are isomorphic.*

A p-rowed square matrix A with elements in $\mathfrak{F}$ is called a multiplication of Ω if

$$\alpha_1 \omega_1 = \omega_1 A, \qquad \alpha_2 \bar{\omega}_2 = \bar{\omega}_2 A, \tag{116}$$

where α_1 and α_2 are matrices. Then (115) is equivalent to

$$\Omega A \Omega^{-1} = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}, \tag{117}$$

and hence to $\Omega A \Omega^{-1} E_r = E_r \Omega A \Omega^{-1}$, $AR_\Omega = R_\Omega A$. The converse is obvious and we have

THEOREM 44. *The multiplication algebra of R_Ω coincides with that of Ω.*

We shall call Ω a *pure Omega matrix* if its multiplication algebra $\mathfrak{D}$ is a division algebra. Hence Ω is pure if and only if R_Ω is irreducible.

2. **The $\mathfrak{F}$-algebra of an irreducible R_Ω.** If R_Ω is an irreducible Weyl matrix with principal matrix C then $-R_\Omega$ is an irreducible Weyl matrix with principal matrix $-C$, the same unit i_0 as R_Ω and index $p - r$. In fact

$$-R_\Omega = i_0 (\Omega^U)^{-1} E_{p-r} \Omega^U, \qquad \Omega^U = H\Omega = \begin{pmatrix} \bar{\omega}_2 \\ \omega_1 \end{pmatrix}, \tag{118}$$

where

$$H = \begin{pmatrix} 0 & I_{p-r} \\ I_r & 0 \end{pmatrix}, \qquad H^{-1} = \begin{pmatrix} 0 & I_r \\ I_{p-r} & 0 \end{pmatrix}, \qquad H^{-1} E_{p-r} H = -E_r. \tag{119}$$

Let $A_1 R_\Omega = R_\Omega A_2$ where A_1 and A_2 have elements in $\mathfrak{F}$ and $A_1 \neq A_2$. Then $R_\Omega A_1 (R_\Omega)^2 = (R_\Omega)^2 A_2 R_\Omega$ so that $A_2 R_\Omega = R_\Omega A_1$ and if

$$A = \tfrac{1}{2}(A_1 + A_2), \qquad N = \tfrac{1}{2}(A - A_1) \neq 0, \tag{120}$$

then $AR_\Omega = R_\Omega A$, $NR_\Omega = -R_\Omega N$. By Theorem 33 the matrix N is non-singular and if $N_1 R = -RN$, then $N_1 N^{-1}$ is in $\mathfrak{D}$. Moreover N^2 and NAN^{-1} are in $\mathfrak{D}$ for every A of $\mathfrak{D}$ so that the $\mathfrak{F}$-algebra of R_Ω is $\mathfrak{D} + \mathfrak{D}N$. But $-R_\Omega$ has index $p - r$ and can be isomorphic to R_Ω only when $p = 2r$. We have

THEOREM 45. *The multiplication algebra $\mathfrak{D}$ of R_Ω is its $\mathfrak{F}$-algebra $\mathfrak{A}$ if and only if R_Ω and $-R_\Omega = R_{\Omega^U}$ are not isomorphic. If $\mathfrak{A} \neq \mathfrak{D}$ so that $-R_\Omega = NR_\Omega N^{-1}$ then $p = 2r$ and $\mathfrak{A} = \mathfrak{D} + \mathfrak{D}N$.*

It is well known[54] that $\mathfrak{A} = \mathfrak{D} + \mathfrak{D}N$ is a division algebra if and only if there exists no A in $\mathfrak{D}$ such that $(AN)^2 = 1$. If N satisfies $NR_\Omega N^{-1} = -R_\Omega$ so does $AN = E$ and, by Theorem 43, we have

THEOREM 46. *There exists a matrix E with elements in $\mathfrak{F}$ such that*

$$E^2 = I_{2r}, \qquad \nu_1\omega_1 = \bar{\omega}_2 E, \qquad \nu_2\bar{\omega}_2 = \omega_1 E, \tag{121}$$

if and only if the $\mathfrak{F}$-algebra of R_Ω is not a division algebra.

3. **Associated matrices** R_Ω. We shall prove

THEOREM 47. *Let R_Ω and R_{Ω_0} be non-isomorphic irreducible Weyl matrices with the same order p, unit i_0, and index r. Then R_Ω and R_{Ω_0} are associated in $\mathfrak{F}$ if and only if $p = 2r$ and R_{Ω_0} is isomorphic to $-R_\Omega$.*

For let $AR_\Omega = R_{\Omega_0}B$ so that $R_{\Omega_0}A(R_\Omega)^2 = (R_{\Omega_0})^2BR_\Omega$ and $BR_\Omega = R_{\Omega_0}A$. Then $(A + B)R_\Omega = R_{\Omega_0}(B + A)$. Since R_Ω is irreducible and not isomorphic to R_{Ω_0}, Theorem 33 states that $A + B = 0$, $B = -A$, $-AR_\Omega = R_{\Omega_0}A$, A is non-singular, and R_{Ω_0} is isomorphic to $-R_\Omega$. By Theorem 43 and our proof that the index of $-R_\Omega$ is $p - r$ we have $p = 2r$. The converse is obvious.

We note finally that if R_{Ω_0} and R_Ω are associated then either Ω_0 is isomorphic to Ω or to Ω_U defined by (117).

VI. Real Riemann Matrices

1. **Riemann matrices over** $\mathfrak{F}$. Let $\mathfrak{F}$ be a real field, $p = 2r$ and

$$\Omega = \begin{pmatrix} \omega \\ \bar{\omega} \end{pmatrix} \tag{122}$$

be an Omega matrix over $\mathfrak{F}$ with principal matrix $C = -C'$. Then we call ω a Riemann matrix over $\mathfrak{F}$ and define $R_\omega \equiv R_\Omega$. It is evident that $i_0 = i$, $\gamma_2 = \bar{\gamma}_1$ in (105), so that the second condition of (105) is redundant. Then our present definition is the direct generalization to a real field $\mathfrak{F}$ of the Lefschetz[55] formulation of a definition of Riemann matrices over the field of all rational numbers.

It was in the present environment that Weyl first considered[56] his matrices R with the property $R^2 = -I_p$. Weyl did not however give the relation between R_ω and ω nor did he consider the problem of determining ω when R_ω is given. We shall solve this problem. We prove

THEOREM 48. *Let $\mathfrak{F}$ be real, $R^2 = -I_p$, and R be a Weyl matrix over $\mathfrak{F}$ with principal matrix $C = -C'$. Then there exists a Riemann matrix ω over $\mathfrak{F}$ with principal matrix C and such that $R = R_\omega$ if and only if R is real.*

For C is non-singular and skew-symmetric so that p is even and it is known that there exists a matrix A with elements in $\mathfrak{F}$ such that

$$ACA' = \begin{pmatrix} 0 & I_r \\ -I_r & 0 \end{pmatrix}, \qquad p = 2r, \tag{123}$$

[54] Cf. Albert (10).
[55] Lefschetz (4).
[56] Weyl (2).

and hence

$$(124) \qquad \begin{pmatrix} I_r & iI_r \\ I_r & -iI_r \end{pmatrix} AC_0A' \begin{pmatrix} I_r & I_r \\ -iI_r & iI_r \end{pmatrix} = 2\begin{pmatrix} I_r & 0 \\ 0 & -I_r \end{pmatrix}.$$

Then C_0 has index r so that R has index $r = \frac{1}{2}p$.

If $R = R_\omega$ then $\gamma = i\omega C\bar{\omega}' = \bar{\gamma}'$ is positive definite Hermitian, $\omega_0 = \gamma^{-1}i\omega C$ is a Riemann matrix isomorphic to ω, and

$$(125) \qquad \Omega^{-1} = (\bar{\omega}_0', \omega_0').$$

Then

$$(126) \qquad R_\omega = i[\bar{\omega}_0'\omega - \overline{(\bar{\omega}_0'\omega)}]$$

is evidently real. Conversely let R be real so that $R = R_{\Omega_0}$ where Ω_0 is given by (105). Since $i_0 = i$ equations (106) imply that $\omega \equiv \omega_1$ is a Riemann matrix over $\mathfrak{F}$ and hence Ω given by (122) is non-singular. Consider the equation

$$(127) \qquad \Omega_0 R = iE_r\Omega_0,$$

and obtain $\omega_1 R = i\omega_1$. Then $\omega R = i\omega$ and the hypothesis that R is real implies also that $\bar{\omega}R = -i\bar{\omega}$ so that

$$(128) \qquad \Omega R = iE_r\Omega, \qquad R = R_\omega,$$

as desired. We note that

$$(129) \qquad \Omega_0^{-1}E_r\Omega_0 = i^{-1}R = \Omega^{-1}E_r\Omega$$

implies that

$$(130) \qquad \omega_2 = \alpha\omega$$

is a Riemann matrix isomorphic with ω.

It is customary to call a p-rowed and $2p$ columned Riemann matrix *a Riemann matrix of genus p. We shall use this convention henceforth* and then have R_ω a *square matrix of $2p$ rows.*

If ω and ω_0 are Riemann matrices of genus p and $R_\omega = R_{\omega_0}$ then $\Omega^{-1}E_p\Omega = \Omega_0^{-1}E_p\Omega_0$, $\Omega_0\Omega^{-1}$ is commutative with E_p and hence

$$(131) \qquad \begin{pmatrix} \omega_0 \\ \bar{\omega}_0 \end{pmatrix} = \Omega_0 = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}\begin{pmatrix} \omega \\ \bar{\omega} \end{pmatrix}, \qquad \omega_0 = \alpha\omega.$$

Conversely if $\omega_0 = \alpha\omega$ then

$$(132) \qquad \Omega_0\Omega^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}$$

is commutative with E_p so that $R_\omega = R_{\omega_0}$. If $R_\omega = -R_{\omega_0}$ then $\Omega_0\Omega^{-1}E_p = -E_p\Omega_0\Omega^{-1}$ and

$$(133) \qquad \Omega_0 = \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix}\begin{pmatrix} \omega \\ \bar{\omega} \end{pmatrix}, \qquad \omega_0 = \alpha\bar{\omega},$$

and conversely.

THEOREM 49. *Let ω and ω_0 be Riemann matrices of the same genus p. Then $R_{\omega_0} = \pm R_\omega$ if and only if $\omega_0 = \alpha\omega$, or $\omega_0 = \alpha\bar{\omega}$, respectively.*

We have therefore proved that the solutions ω of $R_\omega = \pm R$ are essentially unique. Note that the matrix

$$\Delta_0 = \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}, \tag{134}$$

is isomorphic to

$$\Delta = (R_\omega, iIp), \tag{135}$$

since if

$$B = \begin{pmatrix} I_p & I_p \\ -I_p & I_p \end{pmatrix}, \tag{136}$$

then

$$i\,\Omega\Delta = (E_p\,\Omega, \Omega) = \begin{pmatrix} \omega & \omega \\ -\bar{\omega} & \bar{\omega} \end{pmatrix} = \Delta_0 B. \tag{137}$$

3. **Real Riemann matrices.** A Riemann matrix ω of genus p is called real if

$$\lambda\,\omega = \bar{\omega}\,L, \qquad L^2 = I_{2p}, \tag{138}$$

where L has elements in $\mathfrak{F}$. Theorem 46 may now be restated as

THEOREM 50. *A pure Riemann matrix ω is real if and only if the $\mathfrak{F}$-algebra of R_ω is not a division algebra.*

By (138), $\bar{\lambda}\bar{\omega} = wL$ and

$$\begin{pmatrix} 0 & \lambda \\ \bar{\lambda} & 0 \end{pmatrix} = \Omega L \Omega^{-1}, \qquad \begin{pmatrix} \lambda\bar{\lambda} & 0 \\ 0 & \bar{\lambda}\lambda \end{pmatrix} = \Omega L^2 \Omega^{-1} = I_{2p}. \tag{139}$$

But then if

$$\mu = \begin{pmatrix} I_p & \lambda \\ I_p & -\lambda \end{pmatrix}, \qquad \mu^{-1} = \tfrac{1}{2}\begin{pmatrix} I_p & I_p \\ \bar{\lambda} & -\bar{\lambda} \end{pmatrix}, \tag{140}$$

the matrix L is similar in Γ to

$$\begin{aligned}(\mu\Omega)L(\mu\Omega)^{-1} &= \mu\begin{pmatrix} 0 & \lambda \\ \bar{\lambda} & 0 \end{pmatrix}\mu^{-1} = \tfrac{1}{2}\begin{pmatrix} I_p & \lambda \\ -I_p & \lambda \end{pmatrix}\begin{pmatrix} I_p & I_p \\ \lambda & -\bar{\lambda} \end{pmatrix} \\ &= \begin{pmatrix} I_p & 0 \\ 0 & -I_p \end{pmatrix} = E_p.\end{aligned} \tag{141}$$

It follows that E_p is similar in $\mathfrak{F}$ to $L = AE_pA^{-1}$ where A has elements in $\mathfrak{F}$

and $\omega_0 = \omega A$ is isomorphic to ω and has the property $\lambda\omega_0 = \bar{\omega}_0 E_p$. Hence we may rewrite (138) as

$$\lambda\omega = \bar{\omega}E\,, \qquad E = E_p = \begin{pmatrix} I_p & 0 \\ 0 & -I_p \end{pmatrix}. \tag{142}$$

Let C_0 be a principal matrix of ω and write

$$\omega = (\omega_1, \omega_2),\ C_0 = \begin{pmatrix} C_1 & C_2 \\ -C_2' & C_3 \end{pmatrix}, \qquad C_0E = \begin{pmatrix} C_1 & -C_2 \\ -C_2' & -C_3 \end{pmatrix}, \tag{143}$$

where $\omega_1, \omega_2, C_1, C_2, C_3$ are p-rowed square matrices. Our definition of a Riemann matrix gives

$$(\omega C_0)\omega' = (\omega_1 C_1 - \omega_2 C_2')\,\omega_1' + (\omega_1 C_2 + \omega_2 C_3)\,\omega_2' = 0\,, \tag{144}$$

whence

$$\pi = (\omega_1 C_2 + \omega_2 C_3)\,\omega_2' = (\omega_2 C_2' - \omega_1 C_1)\,\omega_1'\,. \tag{145}$$

Evidently $E^{-1} = E' = E$, $i\omega C_0\bar{\omega}' = i\omega C_0(\lambda\omega E)' = i\omega(C_0E)\omega'\lambda\omega$ is positive definite and

$$\omega(C_0E)\omega' = (\omega_1 C_1 - \omega_2 C_2')\,\omega_1' - (\omega_1 C_2 + (\omega_2 C_3)\,\omega_2' = -2\pi \tag{146}$$

is non-singular. Our definition (145) of π states that ω_1 and ω_2 are also non-singular.

The matrix ω is isomorphic to $\omega_0 = i\omega_2^{-1}\,\omega = (S, iI_p)$ where $S = i\omega_2^{-1}\omega_1$. But $\lambda(\omega_1, \omega_2) = (\bar{\omega}_1, \bar{\omega}_2)E$ and $\lambda\omega_1 = \bar{\omega}_1$, $\lambda\omega_2 = -\bar{\omega}_2$, $\lambda = -\bar{\omega}_2\omega_2^{-1} = \bar{\omega}_1\omega_1^{-1}$, $\overline{\omega_2^{-1}\omega_1} = -\omega_2^{-1}\omega_1$ is pure imaginary. Hence S is real and we have proved that every real Riemann matrix is isomorphic to $\omega = (S, iI_p)$ where S is real and non-singular, and $\bar{\omega} = \omega E$.[57]

We next show that *if* C_0 *of* (143) *is a principal matrix of* $\omega = (S, iI_p)$ *then so is*

$$\begin{pmatrix} 0 & C_2 \\ -C_2' & 0 \end{pmatrix}. \tag{147}$$

For we compute

$$R_\omega = i\Omega^{-1}E\Omega = i\Omega^{-1}\begin{pmatrix} I_p & 0 \\ 0 & -I_p \end{pmatrix}\begin{pmatrix} S & iI_p \\ S & -iI_p \end{pmatrix} \tag{148}$$

$$= \tfrac{1}{2}\,i\begin{pmatrix} S^{-1} & S^{-1} \\ -iI_p & iI_p \end{pmatrix}\begin{pmatrix} S & iI_p \\ -S & iI_p \end{pmatrix} = \begin{pmatrix} 0 & -S^{-1} \\ S & 0 \end{pmatrix}$$

and have

$$\tau_0 = R_\omega C_0 = \begin{pmatrix} 0 & -S^{-1} \\ S & 0 \end{pmatrix}\begin{pmatrix} C_1 & C_2 \\ -C_2' & C_3 \end{pmatrix} = \begin{pmatrix} S^{-1}C_2' & -S^{-1}C_3 \\ SC_1 & SC_2 \end{pmatrix} \tag{149}$$

---

[57] An analogous form was obtained by S. Cherubino (1). His form may be derived from the form $(\omega_1, \omega_2 i)$ of S. Lefschetz (2) by our above proof that ω_1, ω_2 are non-singular.

positive definite by Theorem 48. But then SC_2 and $S^{-1}C_2'$ are positive definite and (147) is a principal matrix of R_ω and hence of ω. Since τ_0 is real the matrix $\tau = SC_2$ is a positive definite real symmetric matrix.

We have $\omega = (S, iI_p)$,

$$(S, iI_p)\begin{pmatrix} C_2 & 0 \\ 0 & I_p \end{pmatrix} = (\tau, iI_p) \tag{150}$$

where τ is a real Weyl matrix over $\mathfrak{F}$. If $\sigma = G\,\tau\,H$ is any Weyl matrix associated with τ then ω is isomorphic to

$$G\,(\tau, iI_p)\begin{pmatrix} H & 0 \\ 0 & G^{-1} \end{pmatrix} = (\sigma, iI_p) \tag{151}$$

By Theorem 31 we may take $\tau = RC$ where $C = C'$ and *R is a central Weyl matrix.* We have

THEOREM 51. *Let ω be a real Riemann matrix of genus p over $\mathfrak{F}$. Then there exists a positive definite real symmetric p-rowed matrix $\tau = RC$, where $C = C'$ has elements in $\mathfrak{F}$, and R is a central Weyl matrix, such that ω is isomorphic to (σ, iI_p) where σ is any Weyl matrix associated with R. In particular ω is isomorphic to*

$$\omega_\tau = (\tau, iI_p)\,, \qquad \omega_R = (R, iI_p) = \omega_\tau\begin{pmatrix} C^{-1} & 0 \\ 0 & I_p \end{pmatrix}, \tag{152}$$

with principal matrices

$$\begin{pmatrix} 0 & I_p \\ -I_p & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & C \\ -C & 0 \end{pmatrix} \tag{153}$$

respectively. Conversely $\omega_\tau = \bar{\omega}_\tau\, E$ and $\omega_R = \bar{\omega}_R E$ are isomorphic real Riemann matrices.

4. **Reduction theory.** We shall henceforth use the canonical form $\omega = (R, iI_p)$, where R is a central Weyl matrix, whenever we discuss real Riemann matrices.

Let R be irreducible and $\mathfrak{D}$ be the multiplication algebra of R. If A ranges over all quantities of $\mathfrak{D}$ the set of matrices

$$a_A = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \tag{154}$$

form an algebra $\mathfrak{D}_0$ equivalent to $\mathfrak{D}$. Since $A\omega = \omega a_A$ the multiplication algebra $\mathfrak{A}$ of ω has $\mathfrak{D}_0$ as a sub-algebra. We shall prove

THEOREM 52. *The multiplication algebra $\mathfrak{A}$ of ω is $\mathfrak{D}_0$ or the algebra $\mathfrak{A}$ of Theorem 38 according as R is not or is associated with R^{-1}.*

For let $\alpha = \alpha_1 + \alpha_2 i$ where α_1 and α_2 are real and $\alpha\omega = \omega a$, a has elements

in $\mathfrak{F}$. We compute

$$(155)\qquad a = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \qquad \alpha R = RA_1 + iA_3, \qquad \alpha i = RA_2 + iA_4,$$

and hence have $\alpha_1 = A_4$, $\alpha_2 = -RA_2$, $\alpha_1 R = A_4 R = RA_1$, $-RA_2R = A_3$. If R is not associated with R^{-1} then $RA_2 = -A_3R^{-1}$ implies that $A_2 = A_3 = 0$ be Theorem 33. Moreover R is a central Weyl matrix so that $A_1 = A_4 = A$ is in $\mathfrak{D}$ and $a = a_A$, $\mathfrak{A} = \mathfrak{D}_0$. If R is associated with R^{-1} then we put $GR^{-1} = RH$ as in (88) and have g defined as in (93),

$$(156)\qquad (-RHi)\,\omega = \omega \begin{pmatrix} 0 & H \\ -G & 0 \end{pmatrix} = \omega G.$$

But $-A_3R^{-1} = RA_2$ so that as in the proof of (89), $A_3 = -BG$, $A_2 = BH$ with B in $\mathfrak{D}$. Also $A_1 = A_4 = A$ in $\mathfrak{D}$ and

$$(157)\qquad a = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} + \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} g$$

is in $\mathfrak{A}$. Thus $\mathfrak{A}$ is the algebra of Theorem 38. We now prove

THEOREM 53. *Let ω be given as in the hypotheses of Theorem 52 and $\omega_0 = (S, iI_p)$ where S is a Weyl matrix. Then ω is isomorphic to ω_0 if and only if S is associated with either R or R^{-1}.*

For let $\alpha\omega = \omega_0 a$ and $a \neq 0$ have the notation of (155). Then $\alpha R = SA_1 + iA_3$, $\alpha i = SA_2 + iA_4$, $\alpha = \alpha_1 + \alpha_2 i$. Hence $\alpha_1 R = SA_1$, $\alpha_2 R = A_3$, $\alpha_1 = A_4$, $\alpha_2 = -SA_2$, $A_4R = SA_1$, $-SA_2R = A_3$, $SA_2 = -A_3R^{-1}$. If S is not associated with either R or R^{-1} then Theorem 33 states that $A_2 = A_3 = A_4 = A_1 = 0$, $a = 0$, contrary to hypothesis. Conversely if $A_4R = SA_1$ then A_4 and A_1 are non-singular and $A_4\omega = \omega_0 a$ where A_4 and a are non-singular, $A_2 = A_3 = 0$, ω is isomorphic to ω_0. On the other hand if $-SA_2R = A_3$ then $-SA_2 i\omega = \omega_0 a$ with A_2, A_3, a non-singular, ω is isomorphic to ω_0.

A real Riemann matrix ω will be called *irreducible* if ω is isomorphic to (R, iI_p) where R is an irreducible central Weyl matrix. If ω is also isomorphic to (R_0, iI_p) where R_0 is a Weyl matrix then we have proved that R_0 is associated with either R or R^{-1} and hence has the same $\mathfrak{F}$-algebra as R. But then $\omega_0 = (R_0, iI_p)$ is irreducible if and only if the $\mathfrak{F}$-algebra of R_0 is a division algebra. We now prove the

ANALOGUE OF THE POINCARÉ THEOREM. *Every real Riemann matrix ω is isomorphic to*

$$(158)\qquad \begin{bmatrix} \omega_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \omega_s \end{bmatrix}$$

where the ω_i are irreducible real Riemann matrices which are either equal or non-isomorphic.

For let $\omega = (R, iI_p)$ where R is a central Weyl matrix. By Theorems 34, 51 we may take

$$(159) \qquad R = \begin{bmatrix} R_1 & & \\ & \ddots & \\ & & R_s \end{bmatrix}$$

where the R_i are either equal or not associated and are irreducible central Weyl matrices. Then ω is obviously also isomorphic to (158) where $w_j = (R_j, iI_{p_j})$ and if $\omega_j \neq \omega_k$ then ω_j is not isomorphic to ω_k by Theorem 52 unless $\omega_k = (R_j^{-1}, iI_p)$. In this case we again replace ω_k by ω_j and have $\omega_r = \omega_j$.

The above reduction of ω is an essentially unique one and will provide a unique reduction of any real Riemann matrix to pure components when we have a reduction of an *irreducible impure real Riemann matrix to its pure components.* This is provided by

THEOREM 54. *An irreducible real Riemann matrix is impure if and only if it is isomorphic to a matrix*

$$(160) \qquad \begin{pmatrix} \omega_1 & 0 \\ 0 & \bar{\omega}_1 \end{pmatrix},$$

where ω_1 is pure and not a real Riemann matrix.

For let $\omega = (R, iI_p)$ where R is an irreducible central Weyl matrix and ω is impure. By Theorem 40 and 41 the multiplication algebra of ω is either $\mathfrak{D}_1 \oplus \mathfrak{D}_2$ or $\mathfrak{B} \times \mathfrak{M}_2$. In either case ω is isomorphic to

$$(161) \qquad \omega_0 = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix} = \rho\omega G,$$

where ω_1 and ω_2 are pure and are non-isomorphic or isomorphic in the two above respective cases. When $\bar{\omega}_0 = \bar{\rho}\bar{\omega}G = \bar{\rho}\omega EG = \bar{\rho}\rho^{-1}\omega_0 G^{-1} EG$ so that $\lambda\bar{\omega}_0 = \bar{\omega}_0 L$ where $L = G^{-1}EG$. But then ω_0 is a real Riemann matrix and

$$(162) \qquad \lambda\bar{\omega}_0 = \begin{pmatrix} \lambda_1\bar{\omega}_1 & \lambda_2\bar{\omega}_2 \\ \lambda_3\bar{\omega}_1 & \lambda_4\bar{\omega}_2 \end{pmatrix} = \omega_0 L = \begin{pmatrix} \omega_1 L_1 & \omega_1 L_2 \\ \omega_2 L_3 & \omega_2 L_4 \end{pmatrix}.$$

If $L_2 = L_3 = 0$ then $L_1^2 = I_{2p_1}, L_4^2 = I_{2p_2}$ and $\lambda_1\bar{\omega}_1 = \omega_1 L_1$, $\lambda_4\bar{\omega}_2 = \omega_2 L_4$. The matrices ω_1, ω_2 are real and are isomorphic to (R_1, iI_p) (R_2, iI_p) and ω is isomorphic to (S, iI_p) where

$$(163) \qquad S = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}$$

is ***reducible***. This is impossible by Theorem 49.

Hence L_2 or L_3 is not zero and $\mu\bar{\omega}_1 = \omega_2 M$ with $M \neq 0$. It is well known[58] that then μ and M are non-singular and ω_2 is isomorphic to $\bar{\omega}_1$. Hence ω is isomorphic to (161). By Theorem 46 the matrix ω_1 is not real since R is associated with R_{ω_1} by (118), (120). The converse is an immediate consequence of Theorem 46.

We have therefore completely determined the structure of real Riemann matrices in terms of their pure components. We also gave *a complete treatment of the multiplication algebra of a pure real Riemann matrix* in Section 6 of Chapter IV. We pass now to a study of the existence of Weyl matrices and pure real Riemann matrices with a given multiplication algebra.

VII. Existence Theorems

1. **Representation theory.** A simple algebra $\mathfrak{A}$ of order h over $\mathfrak{F}$ has the form[59]

$$\mathfrak{A} = \mathfrak{M}_s \times \mathfrak{D} \tag{164}$$

where $\mathfrak{M}_s$ is a total matric algebra of degree s and $\mathfrak{D}$ is a normal division algebra of degree n over the centrum $\mathfrak{K}$ of $\mathfrak{A}$. The field $\mathfrak{K} = \mathfrak{F}(k)$ where k satisfies

$$\phi(\lambda) = \lambda^t - a_1\lambda^{t-1} - \cdots - a_t = 0 \qquad (a_1, \cdots, a_t \text{ in } \mathfrak{F}), \tag{165}$$

irreducible in $\mathfrak{F}$, and[60]

$$h = s^2n^2t \tag{166}$$

We let $\mathfrak{A}$ *be an algebra of p-rowed square matrices with elements in* $\mathfrak{F}$.

The matrix k has an irreducible minimum equation $\phi(\lambda) = 0$ and $p = tp_0$,[61]

$$k_0 = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_t \\ 1 & 0 & & \cdot & \cdot \\ 0 & 1 & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & 1 & a_1 \end{bmatrix}, \qquad k = \begin{bmatrix} k_0 & & \\ & \ddots & \\ & & k_0 \end{bmatrix} = k_0 \times I_{p_0}. \tag{167}$$

Thus the set of all p-rowed square matrices commutative with k forms a total matric algebra with elements in $\mathfrak{F}(k_0) \times I_{p_0} = \mathfrak{K}$. In particular $\mathfrak{A}$ is a subalgebra of $\mathfrak{M}_{p_0}$ over $\mathfrak{K}$ and

$$\mathfrak{M}_{p_0} = \mathfrak{M}_s \times \mathfrak{D} \times \mathfrak{D}^{-1} \times \mathfrak{M}_\pi, \tag{168}$$

where $\mathfrak{D}^{-1}$ is reciprocal to $\mathfrak{D}$. Thus

$$p = tsn^2\pi. \tag{169}$$

[58] Cf. Albert (6).

[59] Cf. Wedderburn (4), p. 159.

[60] Cf. Albert (8), Theorem 11.

[61] A consequence of the theorem which states that the characteristic equation of k is an exact power of its irreducible minimum equation $\phi(\lambda) = 0$.

We wish to construct p-rowed central Weyl matrices R with a given multiplication algebra $\mathfrak{A}$ satisfying the hypotheses of Theorems 27–30. This will not be difficult when R is arbitrary and we shall prove that the condition $p = tsn^2\pi$ is sufficient as well as necessary. When we have the additional complication $R = R_\Omega$ the condition $p = tsn^2\pi$ is known,[62] in the theory of Riemann matrices, to be insufficient in special cases. Hence we shall choose π in a manner as convenient as possible in these more difficult cases.

Let $C = \pm\bar{C}'$, $i_0C = C_0 = \bar{C}_0'$ be Hermitian of index r such that

$$C\bar{A}'C^{-1} = A^T. \tag{170}$$

Then

$$A_1 = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}, \qquad C_1 = \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}, \qquad C_{01} = \begin{pmatrix} C_0 & 0 \\ 0 & C_0 \end{pmatrix},$$

give a representation of $\mathfrak{A}$, C by $2p$-rowed square matrices such that C_{01} has index $2r$ and $C_1\bar{A}_1'C_1^{-1} = A_1^T$. Hence *we may always replace* r *by* $2r$ *in our later discussions by taking the order of* R *sufficiently large.* Moreover we have constructed C so that *the canonical form of* C_0 *is*

$$\begin{bmatrix} e_1 & 0 & 0 & 0 \\ 0 & e_1 & 0 & 0 \\ 0 & 0 & -e_2 & 0 \\ 0 & 0 & 0 & -e_2 \end{bmatrix}, \tag{171}$$

with e_1 and e_2 diagonal matrices with positive elements.

2. **Adjunction of $\mathfrak{K}_0$, $\mathfrak{K}$.** The T-symmetric sub-field $\mathfrak{K}_0$ of the centrum $\mathfrak{K}$ of an algebra $\mathfrak{A}$ of Theorem 27 is a total real extension $\mathfrak{F}_0(S)$ of the real field $\mathfrak{F}_0$. The minimum equation of S has degree u and real roots $\sigma_1, \cdots, \sigma_u$, $p = up_1$,

$$\sigma = \begin{bmatrix} \sigma_1 I_{p_1} & & \\ & \ddots & \\ & & \sigma_u I_{p_1} \end{bmatrix}, \qquad V_S = (\sigma_j^{k-1} I_{p_1}), \qquad (j, k = 1, \cdots, u), \tag{172}$$

and it is well known[63] that $\mathfrak{A}$ has a representation in which

$$V_S S V_S^{-1} = \sigma.$$

The quantities A of $\mathfrak{A}$ are commutative with S whence

$$V_S A V_S^{-1} = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_u \end{bmatrix}, \tag{173}$$

[62] See Albert (7).

[63] Cf. Albert (1).

where the A_j are *conjugate* p_1-rowed square matrices with elements in $\mathfrak{F}_j = \mathfrak{F}(\sigma_j)$ respectively. Similarly

$$V_S R V_S^{-1} = \begin{bmatrix} R_1 & & \\ & \ddots & \\ & & R_u \end{bmatrix}. \tag{174}$$

The assumption that S is T-symmetric is equivalent to $C\bar{S}'C^{-1} = S$ and thus to $\bar{C}' = \epsilon C$, $\epsilon = \pm 1$,

$$V_S C V_S' = \begin{bmatrix} C_1 & & \\ & \ddots & \\ & & C_t \end{bmatrix}, \qquad \bar{C}_i' = \epsilon C_i\,, \tag{175}$$

where the C_j are conjugate matrices. But then $V_S = \bar{V}_S$,

$$V_S \tau \bar{V}_S' = V_S R V_S^{-1} V_S C V_S' = \begin{bmatrix} \tau_1 & & \\ & \ddots & \\ & & \tau_u \end{bmatrix},$$

where $\tau_j = R_j C_j$ is positive definite Hermitian. The matrix R_j is a *Weyl matrix over* $\mathfrak{F}_j$ with principal matrix C_j and $RA = AR$ implies that R_j has $\mathfrak{A}_j$ over $\mathfrak{F}_j$, equivalent to $\mathfrak{A}$ as over $\mathfrak{K}_0$, as a *sub-algebra* of its multiplication algebra.

Conversely let R_j be a central Weyl matrix over $\mathfrak{F}_j$ with principal matrix C_j and *multiplication algebra* $\mathfrak{A}_j$ over $\mathfrak{F}_j$. Then it is easily seen[64] that the matrix R defined by (174) is a Weyl matrix over $\mathfrak{F}$ with principal matrix C defined by (175). Moreover S is in the centrum of the $\mathfrak{F}$-algebra of R *if there exist no matrices* A_{jk}, B_{jk} *with elements in* $\mathfrak{F}_S = \mathfrak{F}(\sigma_1, \cdots, \sigma_u)$ *not all zero such that*

$$A_{jk} R_k = R_j B_{jk} \qquad (j \neq k;\, j, k = 1, \cdots, u). \tag{176}$$

We shall construct central Weyl matrices R_j over $\mathfrak{F}_S$ with C_j as respective principal matrices and $\mathfrak{A}_j$ over $\mathfrak{F}_S$ as multiplication algebras. We shall also make R_j not *pseudo-associated in* $\mathfrak{F}_S$ *with* R_k *for* $j \neq k$. Then (176) will hold only for $A_{jk} = B_{jk} = 0$. The matrices R_j are also Weyl matrices over $\mathfrak{F}_j$ and if A_j and B_j have elements in $\mathfrak{F}_j$ then they have elements in $\mathfrak{F}_S$ so that $A_j R_j = R_j B_j$ implies that $A_j = B_j$ is in $\mathfrak{A}_j$ over $\mathfrak{F}_S$. The only matrices of $\mathfrak{A}_j$ over $\mathfrak{F}_S$ which are in $\mathfrak{F}_j$ are the matrices of $\mathfrak{A}_j$ over $\mathfrak{F}_j$. Thus R_j is a central Weyl matrix over $\mathfrak{F}_j$ with $\mathfrak{A}_j$ over $\mathfrak{F}$ as multiplication algebra.

The matrix R of (174) is now a central Weyl matrix over $\mathfrak{F}$ and has C as principal matrix and $\mathfrak{A}$ as multiplication algebra. For if $AR = RB$ then $V_S A V_S^{-1} V_S R V_S^{-1} = V_S R V_S^{-1} V_S B V_S^{-1}$ and if

$$V_S A V_S^{-1} = (A_{jk})\,, \qquad V_S B V_S^{-1} = (B_{jk})\,, \qquad (j, k = 1, \cdots, u)\,,$$

[64] Cf. the treatment for Riemann matrices in Albert (4).

we have (176) for A_{jk} and B_{jk} with elements in $\mathfrak{F}_S$. Hence $A_{jk} = B_{jk} = 0$ for $j \neq k$, $A_{jj}R_j = R_jB_{jj}$ and $A_{jj} = B_{jj}$ is in $\mathfrak{A}_j$, $A = B$ is in $\mathfrak{A}$.

We have thus reduced the question of the existence of an R over $\mathfrak{F}$ with multiplication algebra $\mathfrak{A}$ to the question of the existence of a set of u matrices $R_1, \cdots, R_u$ over $\mathfrak{F}$ with conjugate (with respect to a sub-field of $\mathfrak{F}$) principal matrices C_i and conjugate multiplication algebras such that R_j is not pseudo-associated in $\mathfrak{F}$ with R_k for $j \neq k$. When R is real so are the R_j and when $R = R_\Omega$ then correspondingly $R_j = R_{\Omega j}$.

If $\mathfrak{F}$ is a real field and $\mathfrak{K} \neq \mathfrak{K}_0$ the centrum of $\mathfrak{A}_i$ is a quadratic extension $\mathfrak{K}_i = \mathfrak{F}_i(\mu_i^{\frac{1}{2}})$, $\mu_i < 0$ in $\mathfrak{F}_i$. When $\mathfrak{F}$ is not a real field then $\mathfrak{F} = \mathfrak{F}_0(\rho)$, $\bar{\rho} = -\rho = \rho^J$, $\mathfrak{K} = \mathfrak{K}_0(\rho)$, so that the centrum of $\mathfrak{A}_i$ is $\mathfrak{F}_i = \mathfrak{F}_0(\sigma_i, \rho)$. Obviously $\mathfrak{K} = \mathfrak{K}_0$ if and only if $\mathfrak{F}$ is real, $\mathfrak{F}_i = \mathfrak{F}(\sigma_i)$ is the centrum of $\mathfrak{A}_i$. Hence $\mathfrak{K}_i \neq \mathfrak{F}_i$ only in the first above case and we have already adjoined $\mathfrak{K}$ except in this case. It is of course sufficient to assume that $\mathfrak{K}_0 = \mathfrak{F}$.

Let $\mathfrak{A} = \mathfrak{F}(Q)$, $Q^2 = \mu I_p$, $\mu < 0$ in $\mathfrak{F}$. Then $p = 2p_0$ and we may choose Q so that

$$(177) \qquad W = \begin{pmatrix} I_{p0} & I_{p0}\mu^{\frac{1}{2}} \\ I_{p0} & -I_{p0}\mu^{\frac{1}{2}} \end{pmatrix}, \qquad Q_0 = WQW^{-1} = \begin{pmatrix} \mu^{\frac{1}{2}} I_{p0} & 0 \\ 0 & -\mu^{\frac{1}{2}} I_{p0} \end{pmatrix}.$$

Since $Q^T = -Q$ we have $CQ'C^{-1} = -Q$, $\bar{Q}_0' = -Q$, $QR = RQ$, and the equivalent conditions

$$(178) \qquad WC\bar{W}' = \begin{pmatrix} C_1 & 0 \\ 0 & \bar{C}_1 \end{pmatrix}, \qquad WRW^{-1} = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}.$$

The matrix R_1 is a Weyl matrix over $\mathfrak{K}_1 = \mathfrak{F}(\mu^{\frac{1}{2}})$ with principal matrix C_1 and similarly for R_2.

We choose R_1 not pseudoisomorphic to R_2 in $\mathfrak{F}(\mu^{\frac{1}{2}})$ and make $\mathfrak{A}_1$ over $\mathfrak{F}(\mu^{\frac{1}{2}}) = \mathfrak{F}_1$ the $\mathfrak{F}_1$-algebra of R_1, $\mathfrak{A}_2$ over $\mathfrak{F}_2 = \mathfrak{F}(-\mu^{\frac{1}{2}}) = \mathfrak{F}_1$ the $\mathfrak{F}_1$-algebra of R_2. Then R of (178) will be a central Weyl matrix over $\mathfrak{F}$ with $\mathfrak{A}$ as multiplication algebra and C of (178) as principal matrix. Moreover we select a set of matrices R^j not pseudoisomorphic in $\mathfrak{F}$ by making the R_1^j and R_2^j not pseudo-isomorphic to both R_1^k and R_2^k for $j \neq k$.

Thus our method of adjunction of $\mathfrak{K}$ gives the same results as for $\mathfrak{K}_0$. But there is a single additional restriction.

When $\mathfrak{F}$ is real and R is real the matrix R_2 of (178) *is the conjugate to R_1 and is not arbitrary.* Hence in this case R_1 must be so chosen that it is not pseudo-isomorphic in $\mathfrak{F}(\mu^{\frac{1}{2}})$ to $\bar{R}_1$.

We note that we first reduced the question of the construction of $C = \pm \bar{C}'$ to that of the C_j and then to that of C_1, $\bar{C}_1$. Hence we need only consider the question of the existence of a C such that $C\bar{A}'C^{-1} = A^T$ for every A of $\mathfrak{A}$ in the case where $\mathfrak{A}$ is a normal simple algebra of p-rowed square matrices with elements in the centrum $\mathfrak{F}$ of $\mathfrak{A}$.

3. **The existence of** C. Let $\mathfrak{A}$ be a J-involutorial simple algebra of p-rowed square matrices with elements in $\mathfrak{F}$, the centrum of $\mathfrak{A}$. We write

$$A = (a_{ij}) \qquad (a_{ij} \text{ in } \mathfrak{F};\, i, j = 1, \cdots, p), \tag{179}$$

and

$$\bar{A}' = (b_{ij}), \qquad b_{ij} = a_{ji}^J \qquad (i, j = 1, \cdots, p), \tag{180}$$

and prove

THEOREM 55. *Let $\mathfrak{A}$ be not a total matric algebra over $\mathfrak{F}_0$. Then there exist two p-rowed square matrices $C_0 = \bar{C}_0'$ and $C = -\bar{C}'$ with elements in $\mathfrak{F}$ such that*

$$A^J = C\bar{A}'C^{-1} = C_0\bar{A}'C_0^{-1}.$$

We write[65] $\mathfrak{M}_p = \mathfrak{A} \times \mathfrak{B}$, $\mathfrak{A} = \mathfrak{D} \times \mathfrak{M}_s$, so that $\mathfrak{B} = \mathfrak{D}^{-1} \times \mathfrak{M}_r$. By Theorem 5 the algebra $\mathfrak{D}$ is J-involutorial and hence so is $\mathfrak{D}^{-1}$ and $\mathfrak{B}$. Then $\mathfrak{M}_p = \mathfrak{A} \times \mathfrak{B}$ possess an involution J in which the sub-algebra $\mathfrak{A}$ is self corresponding. But also $\mathfrak{M}_p$ has the J-centrum preserving involution $A \leftrightarrow \bar{A}'$. By Theorem 4 there exists a non-singular p-rowed square matrix $C = \epsilon\bar{C}'$, $\epsilon = \pm 1$ such that $C\bar{A}'C^{-1} = A^J$ for every A of $\mathfrak{A}$.

If $\mathfrak{F} = \mathfrak{F}_0(\rho)$ and $\bar{\rho} = -\rho$ then $C_0 = \rho C$ has the property $\bar{C}_0' = -\epsilon C_0$. If $\mathfrak{F} = \mathfrak{F}_0$ then $\mathfrak{D}^{-1}$ has degree $r \neq 1$ over $\mathfrak{F}_0$ and contains a quantity a such that $a - a^J = b \neq 0$, $C\bar{b}'C^{-1} = -b$. But $\mathfrak{D}^{-1}$ is a division algebra, b is non-singular and so is $C_0 = bC$. Obviously $C_0\bar{A}'C_0^{-1} = A$ for every A of $\mathfrak{A}$ while $\bar{C}_0' = \epsilon Cb' = -\epsilon bC = -\epsilon C_0$. We have proved Theorem 55.

There remains the case $\mathfrak{A} = \mathfrak{F}_0 \times \mathfrak{M}_s$. In this case we take

$$C = \begin{bmatrix} C_1 & & \\ & \ddots & \\ & & C_1 \end{bmatrix}$$

where $C_1 = \pm\bar{C}_1'$ is an arbitrary non-singular matrix and obviously $C_1 = \bar{C}_1'$ if $s^{-1}p$ is odd.

As a corollary of our above arguments we may now complete Theorem 31. We take $\tau = RC$ and $A\tau = \tau B$. Then $\bar{B}'\tau = \tau\bar{A}'$, and the correspondence $A \leftrightarrow A^T = \bar{B}'$ is an involution T of the $\mathfrak{F}$-algebra $\mathfrak{B}$ of τ. We have proved above that there exists a non-singular matrix $G = \pm\bar{G}'$ such that $A^T = G\bar{A}'G^{-1} = \bar{B}'$ and hence $GAG^{-1} = B$. Put $R_0 = \tau G = R(CG)$ and obtain $AR_0 = \tau(BG) = R_0A$ for every A in the $\mathfrak{F}$-algebra of τ. Thus R is associated with the central Weyl matrix $R_0 = RCG = \tau H^{-1}$ and we may restate Theorem 31 as the

COROLLARY. *Every Weyl matrix R is associated with a central Weyl matrix $R_0 = RCH^{-1}$ where $H = \pm\bar{H}'$ is a principal matrix of R_0.*

[65] This is, as in (166), a consequence of Albert (8), Theorem 11, and Wedderburn (3), (2).

4. **Matrices with a real quaternion algebra of multiplications.** We shall study a real field $\mathfrak{F}$ and a T-involutorial normal division algebra of the first kind over $\mathfrak{F}$. Let $\mathfrak{D}$ be an algebra of Theorem 30 so that there exists a total matric algebra $\mathfrak{M}_s$ such that

$$(181) \qquad \mathfrak{A} = \mathfrak{M}_s \times \mathfrak{D} = Q \times \mathfrak{A}_1 ,$$

where $\mathfrak{A}_1$ is a crossed product defined by a total real galois extension of $\mathfrak{F}$ and Q is the algebra of real quaternions. We assume that $\mathfrak{A}$ is an algebra of p-rowed square matrices with elements in $\mathfrak{F}$,

$$(182) \qquad Q = (I_p, X, Y, XY) , \qquad X^2 = \gamma^2 = -I_p , \qquad YX = -XY ,$$

and have

$$(183) \quad p = n^2\pi s, \quad \mathfrak{M}_p = \mathfrak{M}_s \times \mathfrak{D} \times \mathfrak{D}^{-1} \times \mathfrak{M}_\pi = (Q \times \mathfrak{A}_1) \times (\mathfrak{D}^{-1} \times \mathfrak{M}_\pi) .$$

Theorem 12 states that $n = 2^e \neq 1$ since the extension of $\mathfrak{F}$ to the field Γ_0 of all real numbers of Γ does not split $\mathfrak{A}$. Hence *p is divisible by four.* We also obtained

$$(184) \qquad X^T = -X , \qquad Y^T = -Y ,$$

in our proof of Theorem 30.

Let C_0 be a non-singular p-rowed square matrix with elements in $\mathfrak{F}$ such that $C_0 = \epsilon C_0'$, $\epsilon = \pm 1$,

$$(185) \qquad C_0 A' C_0^{-1} = A^T ,$$

for every A of $\mathfrak{A}$. If we pass to an equivalent representation of $\mathfrak{A}$ such that A goes into $PAP^{-1} = A_P$ then

$$(186) \qquad C_P A_P' C_P^{-1} = (A^T)_P$$

where $C_P = PCP' = \epsilon C_P'$. Hence a given one-to-one representation of $\mathfrak{A}$ by p-rowed matrices with elements in $\mathfrak{F}$ may be replaced by any desired representation.

Write

$$(187) \qquad p = 2\lambda = 4\mu ,$$

and take

$$(188) \quad X = \begin{pmatrix} 0 & I_\lambda \\ -I_\lambda & 0 \end{pmatrix}, \quad V = \begin{pmatrix} I_\lambda & iI_\lambda \\ I_\lambda & -iI_\lambda \end{pmatrix}, \quad \xi = V_0 X V_0^{-1} = \begin{pmatrix} iI_\lambda & 0 \\ 0 & -iI_\lambda \end{pmatrix},$$

where $V_0 \bar{V}_0' = 2I_p$. Then necessarily

$$(189) \quad Y = \begin{pmatrix} y_1 & y_2 \\ y_2 & -y_1 \end{pmatrix}, \qquad V_0 Y V_0^{-1} = \eta = \begin{pmatrix} 0 & Y_1 \\ \bar{Y}_1 & 0 \end{pmatrix}, \qquad Y_1 = y_1 + y_2 i ,$$

where y_1 and y_2 are commutative λ-rowed square matrices such that $y_1^2 + y_2^2 = -I_\lambda$, $Y_1\bar{Y}_1 = -I_\lambda$. Conversely if $Y_1 = Y_1 + Y_2 i$ and

$$Y_1\bar{Y}_1 = -I_\lambda\,, \tag{190}$$

the matrix Y of (189) has the property $YX = -XY$, $Y^2 = -I_p$ and (188), (189) gives a representation of Q. Thus Y_1 is arbitrary except for (190).

The condition $CX'C^{-1} = -X$ is equivalent to

$$C_X = V_0 C \bar{V}_0' = \begin{pmatrix} C_1 & 0 \\ 0 & \bar{C}_1 \end{pmatrix}, \tag{191}$$

with $C_1 = \epsilon\,\bar{C}_1'$ non-singular and with elements in $\mathfrak{F}(i)$. By a simple computation the condition $CY' = -YC$, $(Y')^2 = -I_p$, and hence $C = YCY'$, gives the equivalent condition

$$Y_1\bar{C}_1\bar{Y}_1' = C_1. \tag{192}$$

The quantities of $\mathfrak{A}_1$ are commutative with both X and Y and thus

$$V_0 A V_0^{-1} = \begin{pmatrix} A_1 & 0 \\ 0 & \bar{A}_1 \end{pmatrix}, \qquad \bar{A}_1 = Y_1^{-1} A Y_1\,. \tag{193}$$

But $\mathfrak{A}_1$ is an algebra over $\mathfrak{F}$ and we may thus take A_1 to represent the general quantity of $\mathfrak{A}_1$, A_1 a real matrix. Hence $A_1 = Y_1^{-1}AY$, and $\bar{A}_1 = A_1$. We shall later take the real splitting field Z of Theorem 30 to have a canonical representation and shall then restrict the form of Y_1 accordingly. But Y_1 *will be otherwise arbitrary.*

Consider a central Weyl matrix R with multiplication algebra $\mathfrak{A}$. Then $XR = RX$ implies that

$$R = \begin{pmatrix} S_1 & -S_2 \\ S_2 & S_1 \end{pmatrix}, \qquad V_0 R V_0^{-1} = \begin{pmatrix} R_1 & 0 \\ 0 & R_{11} \end{pmatrix}, \tag{194}$$

where $R_1 = S_1 + S_2 i$ and $R_{11} = S_1 - S_2 i$. Then $YR = RY$ is equivalent to

$$R_{11} = S_1 - S_2 i = Y_1^{-1} R Y_1 = Y_1^{-1}\,(S_1 + S_2 i) Y_1\,. \tag{195}$$

The matrix R_1 is a Weyl matrix of order $\lambda = 2\mu$ with principal matrix $C_1 = Y_1\bar{C}_1\bar{Y}_1'$ and the quantities of $\mathfrak{A}_1$ as multiplications.

Conversely let R_1 be a central Weyl matrix with multiplication algebra $\mathfrak{A}_1$ over $\mathfrak{F}(i)$ and principal matrix $C = Y\bar{C}\bar{Y}'$ where Y is commutative with all of the quantities of $\mathfrak{A}_1$. Then we determine R by $S_1 = R_1 + Y_1^{-1}R_1Y_1$, $S_2 i = R_1 - S_1$ and R is a Weyl matrix with principal matrix C given by (191) since $R_1C_1 = \tau_1$ is positive definite, $Y_1^{-1}R_1Y_1\bar{C}_1 = Y_1^{-1}R_1Y_1Y_1^{-1}C_1(\overline{Y_1^{-1}})' = Y_1^{-1}\,\tau_1(\overline{Y_1^{-1}})'$ is positive definite. The $\mathfrak{F}$-algebra $\mathfrak{B}$ of R has Q as a sub-algebra and thus $\mathfrak{B} = Q \times \mathfrak{B}_1$. If B is in $\mathfrak{B}_1$ then

$$V_0 B V_0^{-1} = \begin{pmatrix} B_1 & 0 \\ 0 & \bar{B}_1 \end{pmatrix}, \qquad \bar{B}_1 = \bar{Y}_1 B_1 Y_1\,, \tag{196}$$

and $B_1R_1 = R_1B_{10}$. But our choise of R_1 implies that B_1 is in $\mathfrak{A}_1$ over $\mathfrak{F}(i)$, B is in $\mathfrak{A}$. Hence R is a central Weyl matrix over $\mathfrak{F}$ with principal matrix C and multiplication algebra $\mathfrak{A}$. *We have therefore reduced the problem of constructing R with multiplication algebra $\mathfrak{A}$ to the problem of constructing R_1 with the given algebra of the second kind $\mathfrak{A}_1$ over $\mathfrak{F}(i)$ and a given C_1 such that $C_1\bar{A}_1'C_1^{-1} = A^T$ for every A_1 of $\mathfrak{A}_1$.* Obviously $\mathfrak{A}_1$ over $\mathfrak{F}(i)$ is a crossed product of Theorem 28 and this present construction is taken care of by our general considerations on matrices R with multiplication algebras of the second kind. Note that *we have not adjoined the centrum of* $\mathfrak{A}$ in the above *but do so when we consider* $\mathfrak{A}_1$ *over* $\mathfrak{F}(i)$, R_1.

If we wish to make R real and hence S_1 and S_2 real the situation becomes more complicated. Here we have $\bar{R}_1 = S_1 - S_2i = Y_1^{-1}R_1Y$. If also $R^2 = \pm I_p$ then also $R_1^2 = \pm I_p$. Thus we shall need to consider more complicated properties in case R is real. We do so later.

5. **Reduction to the case $\mathfrak{A} = \mathfrak{F}$.** Our considerations have now reduced the study of the multiplication algebra $\mathfrak{A}$ of a general central Weyl matrix $\mathfrak{R}$ to the case where $\mathfrak{A}$ is a crossed product over $\mathfrak{F}$ defined by a galois field $Z = \mathfrak{F}(y)$ with conjugate fields $\mathfrak{F}(\alpha_i)$, $(i = 1, \cdots, n)$, such that the α_i are all real. We have $p = n\lambda$ and the representation of $\mathfrak{A}$ may be so chosen that

$$(197)\qquad VyV^{-1} = \begin{bmatrix} \alpha_1 I_\lambda & & \\ & \ddots & \\ & & \alpha_n I_\lambda \end{bmatrix}, \qquad V = (\alpha_i^{j-1} I_\lambda) \qquad (i, j = 1, \cdots, n).$$

Thus

$$(198)\qquad VRV^{-1} = \begin{bmatrix} R_1 & & \\ & \ddots & \\ & & R_n \end{bmatrix}, \qquad Vu_GV^{-1} = \| u_G(\alpha_i, \alpha_j) \| \qquad (i, j = 1, \cdots, n),$$

and $Cy'C^{-1} = y$ gives

$$(199)\qquad VCV' = \begin{bmatrix} C(\alpha_1) & & \\ & \ddots & \\ & & C(\alpha_n) \end{bmatrix}.$$

The condition $yu_G = u_Gy^G$ is equivalent to

$$(200)\qquad u_G(\alpha_i, \alpha_j) = 0 \quad \text{if} \quad \alpha_i \neq \alpha_j^G,$$

so that the matrices Vu_GV^{-1} have only a single non-zero matrix in any row or column. We put

$$(201)\qquad U_G \equiv U_G(\alpha_1) \equiv u_G(\alpha_1^G, \alpha_1).$$

Then $Ru_G = u_G R$ is equivalent to

$$R_i u_G(\alpha_i, \alpha_j) = u_G(\alpha_i, \alpha_j) R_j, \tag{202}$$

and, since the u_G are non-singular matrices,

$$R_i = U_G R_1 U_G^{-1}, \qquad \text{if } \alpha_i = \alpha_1^G, \tag{203}$$

where R_1 is a Weyl matrix over $\mathfrak{F}(\alpha_1)$ with principal matrix C_1.

Conversely let R_1 be a central Weyl matrix over $\mathfrak{F}(\alpha_1)$ with principal matrix C_1 and let R_1 have no non-scalar multiplications, R_i be defined by (203). Then I have shown[66] that the associativity condition of $\mathfrak{A}$ and the equations $u_G u_H = u_{GH} a_{GH}$ imply that the matrix R is commutative with all the quantities of $\mathfrak{A}$. Moreover $u_G^T = (f_G u_G)^{-1}$ where f_G is a total positive quantity of $\mathfrak{F}(y)$ by Theorem 28 and hence $f_G u_G C \bar{u}_G' = C$,

$$f_G(\alpha_i)\, u_G(\alpha_i, \alpha_j)\, C(\alpha_j)\, u_G\overline{(\alpha_i, \alpha_j)}' = C(\alpha_i), \tag{204}$$

whence

$$f_G(\alpha_1^G)\, U_G\, C(\alpha_1)\, \overline{U}_G' = C(\alpha_1^G). \tag{205}$$

The matrix $R_1 C(\alpha_1)$ is positive definite Hermitian so that so is

$$U_G R_1 U_G^{-1} U_G C(\alpha_1) \overline{U}_G' = f_G(\alpha_1^G)^{-1} R_i C(\alpha_i).$$

Then $VRV^{-1}VC\bar{V}'$ is positive definite and hence so is RC. Thus R is a Weyl matrix over $\mathfrak{F}$ with principal matrix C. It is easily seen that our hypothesis that R_1 has only scalar multiplications implies that the $\mathfrak{F}$-algebra of R is its multiplication algebra $\mathfrak{A}$.

Let $\mathfrak{F}_0$ be a field conjugate to $\mathfrak{F}$, $\mathfrak{F}_1$ contain $\mathfrak{F}_0$ and $\mathfrak{F}$, R_0 be a Weyl matrix over $\mathfrak{F}_0$ with principal matrix C_0 and

$$V_0 R_0 V_0^{-1} = \begin{bmatrix} R_{01} & & \\ & \ddots & \\ & & R_{0n} \end{bmatrix}, \qquad R_{0i} = U_{G0} R_{01} U_{G0}^{-1}. \tag{206}$$

Then if A and B have elements in $\mathfrak{F}_1$ such that $AR = R_0 B$ we also have $A_1 R_1 = R_{01} B_1$ where A_1, B_1 have elements in $\mathfrak{F}_1(\alpha_1, \alpha_{10})$ such that $A_1 = B_1 = 0$ implies that $A = B = 0$. If R_{10} is not associated with R_1 then $A = B = 0$.

We now let $\mathfrak{D}$ be a T-involutorial crossed product satisfying the conditions of Theorems 27–30 and with centrum $\mathfrak{K}$ over $\mathfrak{F}$. Then if $\mathfrak{F}_1, \cdots, \mathfrak{F}_t$ are the sub-fields of Γ conjugate to $\mathfrak{K}$ we have reduced the problem of constructing a central Weyl matrix with $\mathfrak{A}$ as multiplication algebra to the problem of constructing t central λ-rowed Weyl matrices $R_1, \cdots, R_t$ with conjugate principal matrices $C_1, \cdots, C_t$ respectively such that R_i has only scalar multiplications in $\mathfrak{F}_i$ and is not associated in the composite $(\mathfrak{F}_i, \mathfrak{F}_j)$ with R_j for $i \neq j$. We shall

[66] Cf. Albert (2) as well as (4), (5).

construct central Weyl matrices R_i over $\mathfrak{F}^0 = (\mathfrak{F}_1, \cdots, \mathfrak{F}_t)$ with principal matrices C_i respectively, with only scalar multiplications, and such that R_i is not associated with R_j in $\mathfrak{F}^0$. Then R_i is obviously a central Weyl matrix over $\mathfrak{F}_i$ and has $\mathfrak{F}_i$ as multiplication algebra. *We have reduced our problem of constructing R to the problem of constructing its components R_i.*

We now consider the difficult case where R is real, $\mathfrak{F}$ is a real field. Suppose first that $\mathfrak{A}$ is an algebra of the second kind so that the adjunction of $\mathfrak{K}_0$ gives

$$V_s R V_s^{-1} = \begin{bmatrix} R_1 & & \\ & \ddots & \\ & & R_t \end{bmatrix}, \tag{207}$$

and the adjunction of $\mathfrak{K}$ gives

$$W_i R_i W_i^{-1} = \begin{pmatrix} S_i & 0 \\ 0 & \bar{S}_i \end{pmatrix}. \tag{208}$$

In this case the $\mathfrak{F}$-algebra of R will have $\mathfrak{K}$ as centrum if S_i is not associated with S_j, $\bar{S}_i$, $\bar{S}_j$. We shall thus take the components R_i of R to be non-associated and such that R_i is not associated with $\bar{R}_i$, $\bar{R}_j$.

Assume next that $\mathfrak{A}$ is an algebra of the first kind with a total real galois splitting field. Then we need only take the components R_i of R to be all real and will have R real. Hence in this case the problem is again reduced to the construction of the R_i. Of course the condition $R^2 = \pm I_p$ is equivalent to $R_i^2 = \pm I_\lambda$ and we shall construct real matrices R_i satisfying these conditions and with only scalar multiplications.

We finally study the case where $\mathfrak{A} = \mathfrak{A}_1 \times Q$ so that

$$V_0 R V_0^{-1} = \begin{pmatrix} S & 0 \\ 0 & \bar{S} \end{pmatrix}, \tag{209}$$

where S is a Weyl matrix of order $\beta = \frac{1}{2}p$ and there exists a β-rowed matrix Y_1 such that $C^{(1)} = Y_1 \overline{C^{(1)} Y_1'}$, $Y_1^{-1} S Y_1 = \bar{S}$, $Y_1 \bar{Y}_1 = -I_\beta$. The matrix $C^{(1)}$ is a principal matrix of S and we wish S to be a central Weyl matrix over $\mathfrak{F}(i)$ with $\mathfrak{A}_1$ over $\mathfrak{F}(i)$ as multiplication algebra. But Y_1 is commutative with all the quantities of $\mathfrak{A}_1$ and hence the adjunction of $\mathfrak{K}_0$ to $\mathfrak{F}(i)$ reduces our construction problem to the existence of sets of matrices of the form S_0 with principal matrix C_0 such that $Y_{10} \bar{Y}_{10} = -I_\lambda$, $Y_{10} \bar{C}_0 \bar{Y}'_{10} = C_0$, $Y_{10}^{-1} S_0 Y_{10} = \bar{S}_0$, and such that $AS_0 = S_{01} B$ if and only if $A = B = 0$. Moreover Y_{10} is commutative with every quantity of $\mathfrak{A}_1$ over $\mathfrak{F}(\sigma_1, i)$ so that

$$V Y_{10} V^{-1} = \begin{bmatrix} Y_1^0 & & \\ & \ddots & \\ & & Y_n^0 \end{bmatrix}, \qquad Y_i^0 = U_G Y_1^0 U_G^{-1}, \tag{210}$$

and

$$
(211) \quad VS^0V^{-1} = \begin{bmatrix} R_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & R_n \end{bmatrix}, \quad (Y_1^0)^{-1}R_1Y_1^0 = \bar{R}_1, \quad Y_1^0\overline{C(\alpha_1)(Y_1^0)'} = C(\alpha_1).
$$

The matrix Y_1^0 is arbitrary save only that $Y_1^0 \bar{Y}_1^0 = -I_\mu$, $2\beta = 2nt\mu = p$ and μ is even. We thus see that the second condition of (210) is a restriction on the U_G, and we need only construct a central Weyl matrix R_1 with a given principal matrix C_1 such that, for a Y_1 at our choice, $Y_1\bar{C}_1\bar{Y}_1' = C_1$, $Y_1^{-1}R_1Y_1 = \bar{R}_1$, R_1 has only scalar multiplications, and then construct other non-associated components in a similar fashion. When $R^2 = \pm I_p$ we must have $R_i^2 = \pm I_p$ and we saw that we can then take the index s of the matrix C_1 to be even, if we desire, by studying matrices R of order $2p$. *We shall use this property in our later construction.*

In a later section we shall show that, in order to study real Riemann matrices and thus real Weyl matrices R associated or not associated with R^{-1}, it is sufficient to study $R^2 = \pm I_p$ or R not associated with R^{-1}. If R_i are the components of R_j and R_i is not associated with R^{-1}, then a trivial computation shows that R is not associated with R^{-1}. Hence we shall also restrict our matrices R_i in this fashion. We pass now to existence theorems.

6. The field $\mathfrak{F}$. The investigation made in previous chapters have lead us to consider a non-modular field $\mathfrak{F}$ contained in an algebraically closed field $\Gamma = \Gamma_0(i)$, Γ_0 real closed, and $i^2 = -1$. If α is in Γ then $\alpha = \alpha_1 + \alpha_2 i$ with α_1 and α_2 in Γ_0. We write $\bar{\alpha} = \alpha_1 - \alpha_2 i$, the conjugate of α, and are studying the case where $\bar{\alpha}$ is in $\mathfrak{F}$ for every α of $\mathfrak{F}$, so that

$$
(212) \qquad \mathfrak{F} = \mathfrak{F}_0 \text{ or } \mathfrak{F}_0(\rho), \qquad \mathfrak{F}_0 < \Gamma_1, \qquad \bar{\rho} = -\rho.
$$

In order to obtain our existence theorems *we shall assume that $\mathfrak{F}_0$ is a Hilbert Irreducibility field.*

Define Λ_0 to be the set of all quantities of Γ_0 which are algebraic with respect to $\mathfrak{F}_0$. Then Λ_0 is an *ordered infinite field* and if $a < 0$ then $-a > 0$; if $a > 0$, $b > 0$ then $a + b > 0$, $ab > 0$ for every a and b of Λ_0. We shall prove

THEOREM 56. *Let $m, t_1, \cdots, t_m$ be any positive integers,*

$$
(213) \qquad 0 \leqq \delta_j < \psi_j \qquad (j = 1, \cdots, m)
$$

be quantities of Λ_0. Then there exist quantities $\lambda_1, \cdots, \lambda_m$ in Λ_0 chosen seriatim so that δ_j, ψ_j may be functions of $\lambda_1, \cdots, \lambda_{j-1}$ such that

$$
(214) \qquad 0 \leqq \delta_j < \lambda_j < \psi_j,
$$

and the products

$$
(215) \qquad \lambda_1^{k_1}\lambda_2^{k_2} \cdots \lambda_m^{k_m} \qquad (k_j = 0, 1, \cdots, 2t_j; \quad j = 1, \cdots, m),
$$

are linearly independent in $\mathfrak{F}$.

We proceed by induction and write $\mathfrak{F}_{0j} = \mathfrak{F}_0(\delta_1, \cdots, \delta_j; \psi_1, \cdots, \psi_j; \lambda_1, \cdots, \lambda_{j-1})$. It is then sufficient to prove the existence of a quantity λ_j in Λ_0 satisfying (214) and such that $1, \lambda_j, \lambda_j^2, \cdots, \lambda_j^{2t_j}$ are linearly independent with respect to $\mathfrak{F}_j$, the composite of $\mathfrak{F}$ and $\mathfrak{F}_{0j}$. By Theorem F1 the fields $\mathfrak{F}_{0j}$, $\mathfrak{F}_j$ are H.I. fields and, since

$$f(x, \xi_i) \equiv x^{2t_j+1} + \xi_0 x^{2t_j} + \cdots + \xi_{2t_j} \tag{216}$$

is irreducible in $\mathfrak{F}_j(\xi_0, \xi_1, \cdots, \xi_{2t_j})$, there exist $\bar{\xi}_0, \cdots, \bar{\xi}_{2t_j}$ in $\mathfrak{F}_0$ such that $f(x) = f(x, \bar{\xi}_i)$ is irreducible in $\mathfrak{F}_j$. The equation $f(x) = 0$ has coefficients in the real closed field Γ_0 and odd degree, and hence a root μ_j in Γ_0. Evidently μ_j is in Λ_0 and $1, \mu_j, \cdots, \mu_j^{2t_j}$ are linearly independent in $\mathfrak{F}_j$. If $\mu_j < 0$ then $-\mu_j > 0$ has the same linear independence properties as μ_j so we may assume $\mu_j > 0$. Evidently $\mu_j \neq \psi_j - \delta_j = \psi_{0j} > 0$ which is in $\mathfrak{F}_j$. If $0 < \mu_j < \psi_{0j}$ we write $\lambda_{0j} = \mu_j$. Otherwise $\mu_j - \psi_{0j} > 0$, $\mu_j^{-1}\psi_{0j} > 0$, whence $\psi_{0j} > \psi_{0j}^2 \mu_j^{-1} = \lambda_{0j}$. In either case the quantity $\lambda_{0j} > 0$ is in Λ_0 and generates $\mathfrak{F}_j(\mu_j)$. Put $\lambda_j = \lambda_{0j} + \delta_j$ so that λ_j is in Λ_0, the quantities $1, \lambda_j, \cdots, \lambda_j^{2t_j}$ are linearly independent in $\mathfrak{F}_j$ and $0 < \lambda_j - \delta_j < \psi_j - \delta_j$, $0 \leqq \delta_j < \lambda_j < \psi_j$ as desired. We have proved Theorem 56.

We shall apply Theorem 56 by the use of the known[67]

LEMMA. *Let*

$$\tau = (\tau_{jk}) \qquad (j, k = 1, \cdots, p), \tag{217}$$

be a Hermitian matrix and let ν *in* Γ_0 *have the property*

$$\nu > (\tau_{jk}\bar{\tau}_{jk})^{\frac{1}{2}} \qquad j \neq k; j, k = 1, \cdots, p). \tag{218}$$

Then if the τ_{jj} *are positive real numbers such that*

$$\tau_{jj} \geqq p!_1\nu, \tag{219}$$

the matrix τ *is positive definite.*

7. Real Weyl matrices with only scalar multiplications. Consider a p-rowed square symmetric matrix (217) and write

$$\lambda_{p(i-1)+j} = \tau_{ij} \qquad (i \leqq j; i, j = 1, \cdots, p). \tag{220}$$

Write $\psi_k = 1$ if $i \neq j$ and $\delta_k = p!$ if $i = j$ and select the λ_k as in Theorem 56 such that $m = \frac{1}{2}p(p+1)$,

$$1, \lambda_k, \lambda_k\lambda_s \qquad (k, s = 1, \cdots, m), \tag{221}$$

are linearly independent in $\mathfrak{F}$. By our above lemma the matrix τ is positive definite.

Consider matrices

$$A = (a_{ij}), \qquad B = (b_{ij}), \qquad C = (C_{ij}), \qquad D = (D_{ij}) \qquad (i, m = 1, \cdots, p),$$

[67] Albert (4), Theorem 6.

with elements in $\mathfrak{F}$. Then we may prove

THEOREM 57. *Let $A\tau - \tau B = \tau C\tau + D$. Then $C = D = 0$, $A = B = aI_p$ where a is in $\mathfrak{F}$.*

For

$$(222) \qquad \sum_{j=1}^{p} a_{ij}\tau_{js} - \sum_{k=1}^{p} \tau_{ik}b_{ks} = \sum_{f,g}^{1,\cdots,p} \tau_{if}C_{fg}\tau_{gs} + d_{is} \qquad (i, s = 1, \cdots, p).$$

By the linear independence of (221) in $\mathfrak{F}$ we have $D = 0$, $\tau C\tau = 0$ so that $C = 0$ since τ is non-singular. If $p = 1$ then $A\tau = \tau B$ implies that $A = B$ is in $\mathfrak{F}$. Hence let $p > 1$ so that we may take $i \neq s$, $\tau_{js} = \tau_{ik}$ only when $i = j$, $s = k$. Then

$$(223) \qquad 0 = (a_{ii} - b_{ss})\,\tau_{ik} + \sum_{j \neq i} a_{ij}\tau_{js} - \sum_{k \neq s} \tau_{ik}b_{ks}$$

is a zero linear combination with coefficients in $\mathfrak{F}$ of distinct λ_k. These coefficients must vanish and hence $a_{ij} = b_{ij} = 0$ for $i \neq j$, A and B are diagonal matrices. Then (222) becomes $a_{ii}\,\tau_{is} = \tau_{is}b_{ss}$ so that $\tau_{is} \neq 0$ implies that $a = a_{11} = b_{22} = a_{ii} = b_{ss}$ and $A = B = aI_p$ as desired.

The following theorem follows almost immediately from Theorem 57.

THEOREM 58. *Let $C = \pm C'$ be any p-rowed non-singular matrix with elements in F. Then there exists a Weyl matrix R with principal matrix C such that*

$$AR - RB = G + RHR,$$

for A, B, G, H with elements in $\mathfrak{F}$, if and only if $G = H = 0$, $A = B = aI_p$ with a in $\mathfrak{F}$. Moreover R is a central Weyl matrix over $\mathfrak{F}$ with $\mathfrak{F}$ as multiplication algebra, is not associated with R^{-1}, and has elements in Λ which may be taken real when C has real elements.

For we take $R = \tau C^{-1}$ so that $AR - RB = G + RHR$ is equivalent to $A\tau - \tau C^{-1}BC = GC + \tau C^{-1}H\tau$. Thus $GC = C^{-1}H = 0$ so that $G = H = 0$ and $A = C^{-1}BC = aI_p$, $B = aI_p$. Since $AR = RB$ if and only if $A = B = aI_p$, and $-G = RHR$ if and only if $G = H = 0$, we have proved Theorem 58.

8. **Weyl matrices R not associated with $\bar{R}$.** Let $\mathfrak{F} = \mathfrak{F}_0(\rho)$, $\bar{\rho} = -\rho$ so that $\mathfrak{F}$ is not a real field. If $p = 1$ then $\tau = \bar{\tau}'$ is real and $\tau = \bar{\tau}$, $a\tau = \bar{\tau}a$ for every a of $\mathfrak{F}$, $aR = \bar{R}(\bar{C}aC^{-1})$ is associated with $\bar{R}$. We wish to prove the existence of Weyl matrices R with the properties of Theorem 58 and not associated with $\bar{R}$. Hence we assume $p > 1$.

Put $2n = p(p-1)$ and let μ_k be chosen in Λ_0 such that

$$(224) \qquad 0 < \mu_k < \tfrac{1}{2}(\rho\bar{\rho})^{-\frac{1}{2}} \qquad (k = 1, \cdots, n),$$

while

$$(225) \qquad 1,\ \mu_k,\ \mu_k\mu_s \qquad (k = 1, \cdots, n),$$

are linearly independent in $\mathfrak{F}$. We also write $\lambda(p-1)i + j = \tau_{ij}$ as before

and choose (221) linearly independent in $\mathfrak{F}^0 = \mathfrak{F}(\mu_1, \cdots, \mu_n)$ and such that

$$0 < \tau_{ij} < \tfrac{1}{2}\,; \qquad p! < \tau_{ij} \qquad (i \neq j;\, i, j = 1, \cdots, p)\,. \tag{226}$$

Consider the Hermitian matrix

$$T = \tau + \sigma\rho = (T_{ij}) \tag{227}$$

where $\sigma = (\sigma_{ij})$ is a real skew-symmetric matrix defined by

$$\sigma_{ii} = 0\,, \qquad \sigma_{ij} = \mu_{p(i-1)+j} = -\sigma_{ji}\,(i < j;\, i = 1, \cdots, p;\, j = 2, \cdots, p)\,. \tag{228}$$

The matrix T has $T_{ij} = \tau_{ij} + \rho\sigma_{ij}$ and absolute values

$$|\, T_{ij} \,| = \tau^2_{i\,j} + (|\, \rho\,|^{\frac{1}{2}}\, \sigma_{ij})^2 < 1 \qquad (i \neq j)\,. \tag{229}$$

By Lemma 1 the matrix T is positive definite and satisfies the properties given by Theorem 57. We now prove

LEMMA 2. *Let $a_1 + a_2\rho = a$ and a_1 and a_2 be linearly independent in $\mathfrak{F}$. Then a and $\bar{a}$ are linearly independent in $\mathfrak{F}$.*

For if $\lambda a + \mu\bar{a} = 0$ then $\bar{\lambda} a + \bar{\mu} a = 0$ whence $\nu a = -\overline{\nu a}$ if $\nu = \lambda + \bar{\mu}$. Write $\nu = \nu_1 + \nu_2\rho$ with real ν_1 and ν_2 and have $\nu_1 a_1 + \nu_2 a_2\, \rho^2 = 0$. Since a_1 and a_2 are linearly independent in $\mathfrak{F}$ we have $\nu_1 = \nu_2 = 0, \nu = 0, \mu = -\bar{\lambda}$, $\lambda a = \overline{\lambda a}$. Put $\lambda = \lambda_1 + \lambda_2\rho$ with λ_1 and λ_2 in $\mathfrak{F}_0$ and have $\lambda_1 a_2 + \lambda_2 a_1 = 0$, $\lambda_1 = 0 = \lambda_2$, $\lambda = 0$ as desired.

We have chosen $T_{ij} = \tau_{ij} + \sigma_{ij}\rho$ with the τ_{ij} and σ_{ij} linearly independent for $i \neq j$. Hence the $T_{ji} = \overline{T}_{ij}$ are linearly independent of the T_{ij} for $i \neq j$ and the p^2 elements of T are now *all distinct and are linearly independent in* $\mathfrak{F}$.

Assume a relation $AT = \overline{T}B$ for $A \neq 0$. Theorem 33 states that A and B are non-singular. We have

$$\overline{T}' = T\,, \qquad AT = T'B\,, \qquad B'T = T'A'\,, \qquad T' = ATB^{-1} = B'T(A')^{-1}\,.$$

Thus $(B'^{-1}A)T = T(A'^{-1}B)$. But T is a matrix for which Theorem 57 holds so that $A'^{-1}B = aI_p$, $B = A'a$ with a in $\mathfrak{F}$. Hence

$$AT = (T'A')a = a(AT)'\,, \qquad (AT)' = a(AT) = a^2(AT)'\,, \qquad a^2 = 1\,,$$

$$a = \pm 1\,, \qquad (AT)' = \pm (AT)\,. \tag{230}$$

We write $A = (a_{ij})$ and (229) becomes

$$\sum_{j=1}^{p} a_{ij}T_{jk} = \pm \sum_{s=1}^{p} a_{ks}T_{si} \qquad (i, k = 1, \cdots, p)\,. \tag{231}$$

Since $p > 1$ we may take $i \neq k$ and the linear independence of the T_{ij} in $\mathfrak{F}$ implies that $a_{ij} = 0$, $A = 0$.

A matrix $R = TC^{-1}$ is not associated with $\bar{R}$ since $AR = \bar{R}B$ is equivalent to $AT = \overline{T}\overline{C}^{-1}BC$, $A = B = 0$. We have proved

THEOREM 59. *Let $\mathfrak{F} = \mathfrak{F}_0(\rho)$, $\bar{\rho} = -\rho$. Then the matrix R may be taken to be not associated with $\bar{R}$ if and only if $p > 1$.*

9. A particular association of R and $\bar{R}$. In Section 4 we found it necessary to consider Weyl matrices R such that $\bar{R} = Y^{-1}RY$. We let $i^2 = -1$, $\mathfrak{F} = \mathfrak{F}_0(i)$, $p = 2\lambda$. Consider a p-rowed non-zero skew-symmetric matrix σ_1 with elements in $\mathfrak{F}_0$ and an Hermitian matrix τ_1 of Theorem 59 so chosen that the matrix

$$S = \begin{pmatrix} \tau_1 & i\sigma_1 \\ i\sigma_1 & \bar{\tau}_1 \end{pmatrix} = \bar{S}' \tag{232}$$

is positive definite. This may be accomplished, as in Lemma 1 and Theorem 56, by taking the diagonal elements of τ_1 to be sufficiently large positive quantities. Write

$$Y = \begin{pmatrix} 0 & -I_p \\ I_p & 0 \end{pmatrix}, \quad \eta = \begin{pmatrix} iI_p & 0 \\ 0 & -iI_p \end{pmatrix}, \quad V = \begin{pmatrix} I_p & iI_p \\ I_p & -iI_p \end{pmatrix} \tag{233}$$

so that

$$V\bar{V}' = 2I_p\,, \qquad VYV^{-1} = \eta\,. \tag{234}$$

Then if $\tau_1 = \tau_2 + \tau_3 i$ we have $\tau_{3'} = -\tau_3$,

$$V^{-1}\begin{pmatrix} \tau_1 & 0 \\ 0 & \bar{\tau}_1 \end{pmatrix} V = \tfrac{1}{2}\bar{V}'\begin{pmatrix} \tau_1 & 0 \\ 0 & \bar{\tau}_1 \end{pmatrix} V = \begin{pmatrix} \tau_2 & \tau_{3'} \\ \tau_3 & \tau_2 \end{pmatrix} = \tau \tag{235}$$

is a real symmetric matrix. But $V\tau V^{-1}$ is evidently commutative with η so that Y is commutative with τ. Then we put $V^{-1}SV = T = \frac{1}{2}\bar{V}'SV$ so that T is positive definite. Evidently

$$V^{-1}\begin{pmatrix} 0 & i\sigma_1 \\ i\sigma_1 & 0 \end{pmatrix} V = \begin{pmatrix} i\sigma_1 & 0 \\ 0 & -i\sigma_1 \end{pmatrix} = i\sigma\,, \qquad Y\sigma = -\sigma Y\,, \tag{236}$$

$$YT = \bar{T}Y\,, \qquad T = \tau + \sigma i\,.$$

It is also obvious that if we write λ_k for the distinct elements of T then $1, \lambda_k$, $\lambda_k\,\lambda_s$ are linearly independent in $\mathfrak{F}$. Hence $AT - TB = G + THT$ for A, B, G, H with elements in $\mathfrak{F}$ if and only if $AT = TB$ and $G = H = 0$. Write $A = A_1 + A_2 i$, $B = B_1 + B_2 i$ and obtain

$$A_1\tau - A_2\sigma = \tau B_1 - \sigma B_2\,, \qquad A_2\,\tau + A_1\sigma = \tau B_2 + \sigma B_1\,. \tag{237}$$

The matrix $A_2\,\sigma - \sigma\,B_2$ has elements in $\mathfrak{F}_0$ and the elements of $A_1\,\tau - \tau B_1$ are linear combinations of the λ_k with coefficients in $\mathfrak{F}$. Hence

$$\overline{A_1\tau} = \overline{\tau B_1}\,, \qquad A_2\,\sigma = \sigma B_2\,, \tag{238}$$

while similarly

$$A_2\tau = \overline{\tau B_2}\,, \qquad A_1\sigma = \sigma\,B_1\,. \tag{239}$$

Then

$$(240) \qquad VA_1V^{-1} = \begin{pmatrix} a_1 & a_2 \\ \bar{a}_2 & \bar{a}_1 \end{pmatrix}, \qquad VB_1V^{-1} = \begin{pmatrix} b_1 & b_2 \\ \bar{b}_2 & \bar{b}_1 \end{pmatrix},$$

where a_1, a_2, b_1, b_2 have elements in $\mathfrak{F}$. Hence

$$(241) \qquad \tfrac{1}{2}\, VA_1\tau V^{-1} = \begin{pmatrix} a_1\tau_1 & a_2\bar{\tau}_1 \\ \bar{a}_2\tau_1 & \bar{a}_1\bar{\tau}_1 \end{pmatrix} = V\tau B_1V^{-1} = \begin{pmatrix} \tau_1 b_1 & \tau_1 b_2 \\ \bar{\tau}_1\bar{b}_2 & \bar{\tau}_1\bar{b}_1 \end{pmatrix}.$$

By Theorem 59 we have $a_1 = b_1 = (\alpha_1 + \alpha_2 i)\, I_p$ and $a_2 = b_2 = 0$. Then $A_1 = a_0 + b_0Y = B_1$ where a_0 and b_0 are in $\mathfrak{F}_0$. The second equation of (239) gives $(a_0 + b_0Y - a_0 + b_0Y)\,\sigma = (2Y)b_0\sigma = 0$. Since $2Y$ is non-singular we have $b_0\sigma = 0$ for b_0 in $\mathfrak{F}_0$. Since $\sigma \neq 0$ we have $b_0 = 0$ and $A_1 = B_1$ is in $\mathfrak{F}_0$. In a similar fashion $A_2 = B_2$ is in $\mathfrak{F}_0$ and $A = B = aI_p$ with a in $\mathfrak{F}$. Our proof gives

THEOREM 60. *The matrix T defined above is a Weyl matrix with the properties of Theorem 58 and such that $\bar{T}Y = YT$.*

As an immediate corollary we obtain

THEOREM 61. *Let $C = \pm \bar{C}'$ be a $2p$-rowed non-singular matrix with elements in $\mathfrak{F}$ such that*

$$(242) \qquad YCY^{-1} = \bar{C}\,.$$

Then the matrix $R = TC^{-1}$ is a Weyl matrix of Theorem 58 with principal matrix C and

$$(243) \qquad YR = \bar{R}Y\,.$$

10. Sets of non-associated Weyl matrices. The Weyl matrices R of Theorem 58 have elements which are algebraic over $\mathfrak{F}_0$. Let R_1 be chosen as in Theorem 58 and let $\mathfrak{F}_1$ be the field obtained by extending $\mathfrak{F}$ by the elements of R_1. We then choose R_2 as in Theorem 58 for the field $\mathfrak{F}_1$. If either

$$(244) \qquad AR_1 - R_2B = G + R_1HR_2\,,$$

or

$$(245) \qquad A\bar{R}_1 - R_2B = G + \bar{R}_1HR_2\,,$$

in case $\mathfrak{F} = \mathfrak{F}_0(\rho)$, while A, B, G, H have elements in $\mathfrak{F}$, then

$$A = B = G = H = 0\,.$$

For AR_1, R_1H, B, G have elements in $\mathfrak{F}_1$ and $(AR_1 - G) = R_2B + (R_1H)R_2$. By Theorem 58 we have $AR_1 = G, -B = R_1H$. Again by Theorem 58 we have $A = G = B = H = 0$. Moreover $\bar{R}_1$ satisfies Theorem 58 when R_1 does and (240) gives $A = B = G = H = 0$.

THEOREM 62. *There exist arbitrarily many Weyl matrices R_j of Theorems 58, 59, 61 such that R_i is not associated with $R_j, \bar{R}_j, R_j^{-1}$ for $i \neq j$.*

We now apply our arguments of Sections 1 — 4 to obtain immediately

THEOREM 63. *Let $\mathfrak{D}$ be a T-involutorial division algebra of degree n over its centrum $\mathfrak{K}$ which has degree t over $\mathfrak{F}$. Then $\mathfrak{D}$ is the multiplication algebra of a central Weyl matrix R of order p over $\mathfrak{F}$ if and only if p is divisible by n^2t and $\mathfrak{D}$ is an algebra of Theorem* 27 *and either* 28, 29, *or* 30.

When $\mathfrak{F}$ is real and $\mathfrak{D}$ is an algebra of the first kind with a total real galois splitting field then our Theorem 58 gives

THEOREM 64. *Let $\mathfrak{F}$ be real and $\mathfrak{D}$ be an algebra of the first kind with a total real galois splitting field. Then the matrix R of Theorem* 63 *may be taken real and not associated with R^{-1}.*

We finally apply Theorems 59, 60 and have

THEOREM 65. *Let $\mathfrak{F}$ be real and $\mathfrak{D}$ be a T-involutorial division algebra. Then there exist real central Weyl matrices R with $\mathfrak{D}$ as multiplication algebra and not associated with R^{-1}.*

We shall pass to matrices R such that $R^2 = \pm I_p$ and hence consider matrices R_Ω.

11. Weyl matrices R_Ω.

We shall construct R_Ω by constructing Ω.

Suppose first that $\mathfrak{F}$ is a real field and $C' = -C$. Then we proved in Theorem 42 that $p = 2r$ and $R_\Omega = R_\omega$ where ω is a Riemann matrix of genus r over $\mathfrak{F}$. Moreover we take

$$\omega = (I_r, T), \qquad T = T' = \tau + \sigma i,$$

where τ and σ are r-rowed symmetric matrices with elements in Γ_0. We take $\tau = (\tau_{ij})$ to be a matrix chosen as in the proof of Theorem 57 and then let $\mathfrak{F}^0 = \mathfrak{F}(\tau_{11}, \cdots, \tau_{rr})$, σ to be a matrix also chosen as in the proof of Theorem 57 but with independence with respect to $\mathfrak{F}^0$. The equation $\alpha\omega = \omega A$ is equivalent to $\alpha = A_1 + TA_2$, $(A_1 + TA_2)T = A_3 + TA_4$ where A_1, A_2, A_3, A_4 are r-rowed square matrices with elements in $\mathfrak{F}$. By the proof of Theorem 57 we have $A_2 = A_3 = 0$, $A_1 = A_4 = aI_r$ with a in $\mathfrak{F}$, $A = aI_r$. Thus ω has only scalar multiplications and R_ω has only scalar multiplications.

Let $\alpha\omega = \bar{\omega}A$ so that $\alpha = A_1 + \bar{T}A_2$, $(A_1 + \bar{T}A_2)T = A_3 + \bar{T}A_4$. Precisely as in the proof of Theorem 57 we have $A_2 = A_3 = 0$. But now A_1 and A_4 are real and $A_1\tau = \tau A_4$, $A_1\sigma = -\sigma A_4$. As before $A_1 = A_4 = aI_r$, $2a\sigma = 0$, $a = 0$, $A = 0$. Hence ω is not isomorphic to $\bar{\omega}$, Ω is not isomorphic to $\bar{\Omega}$ and R_ω is not isomorphic to $-R_\omega$ by Theorem 43. Hence R_ω is a central Weyl matrix by Theorem 45.

By choosing matrices $\omega = \omega_1, \omega_2, \cdots, \omega_m$ and hence matrices $\tau_1, \sigma_1, \tau_2, \sigma_2, \cdots, \tau_m, \sigma_m$ as in our proof of Theorem 61 we may evidently make Ω_j not isomorphic to Ω_i or $\bar{\Omega}_i$ for $i \neq j$, $i, j = 1, \cdots, m$. Each Ω_j is not isomorphic to $\bar{\Omega}_j$ and has principal matrix

$$\begin{pmatrix} 0 & I_r \\ -I_r & 0 \end{pmatrix}, \tag{246}$$

a canonical form for any $C_j = -C_j'$. Thus we may pass to isomorphic matrices Ω_{j0} with arbitrary principal matrices C_j. The matrices R_{ω_j} are real by Theorem 48 and are non-associated by Theorems 47, 33. This gives

THEOREM 66. *Let m and r be positive integers, $C_1, \cdots, C_m$ be non-singular skew-symmetric matrices with $p = 2r$ rows of elements in a real field $\mathfrak{F}$. Then there exist real central Weyl matrices $R_1, \cdots, R_m$ such that R_i has C_i as principal matrix, $\mathfrak{F}$ as multiplication algebra, $R_i^2 = -I_p$, and R_i is not associated with R_j for $i \neq j$ and $i, j = 1, \cdots, m$.*

We next prove

THEOREM 67. *Let m and $p > 2$ be positive integers, $\mathfrak{F}$ be real, and $C_1, \cdots, C_m$ be non-singular p-rowed symmetric matrices with elements in $\mathfrak{F}$ and the same index r. Then the conclusions of Theorem 62 are satisfied except that $R_i^2 = I_p$.*

It is sufficient to take $C_i = E_r$. For every symmetric matrix C_i with elements in $\mathfrak{F}$ has the property $C_i = A_iE_rA_i'$ where A_i has elements in a real field $\mathfrak{F}^0$ obtained from $\mathfrak{F}$ by the adjunction of a finite number of real square roots. Then if Ω_{i0} is a real Omega matrix over $\mathfrak{F}^0$ with only scalar multiplications and E_r as principal matrix the matrix $\Omega_i = \Omega_{i0}A_i^{-1}$ has C_i as principal matrix and is an Omega matrix over $\mathfrak{F}$ with $\mathfrak{F}$ as multiplication algebra. A similar argument reduces all other desired properties of Ω_i to properties of Ω_{i0}. Hence we assume that $C_i = E_r$.

Let

$$(247) \qquad \Omega = \begin{pmatrix} \omega_1 \\ \bar{\omega}_2 \end{pmatrix}, \qquad \omega_1 = (I_r, \pi), \qquad \omega_2 = (-\pi', -I_{p-r}),$$

where π has r rows and $p - r$ columns. Without loss of generality we assume $r > 1$ since $p > 2$. Then

$$(248) \qquad \omega_1 E_r \omega_2' = (I_r, \pi)\begin{pmatrix} I_r & 0 \\ 0 & -I_{p-r} \end{pmatrix}\omega_2' = (I_r, -\pi)\begin{pmatrix} -\pi \\ -I_{p-r} \end{pmatrix} = -\pi + \pi = 0,$$

$$(249) \qquad \gamma_1 = \omega_1 E_r \bar{\omega}_1' = (I_r, -\pi)\begin{pmatrix} I_r \\ \bar{\pi}' \end{pmatrix} = I_r - \pi\bar{\pi}',$$

$$(250) \qquad \gamma_2 = -\bar{\omega}_2 E_r \omega_2' = (\bar{\pi}', -I_{p-r})\begin{pmatrix} -\pi \\ -I_{p-r} \end{pmatrix} = I_{p-r} - \bar{\pi}'\pi.$$

Write $\pi = (\pi_{ij})$ and

$$(251) \qquad \lambda_{(i-1)(p-r)+j} = \pi_{ij}, \qquad (i = 1, \cdots, r; j = 1, \cdots, p - r),$$

and choose the λ_k such that

$$(252) \qquad 1, \lambda_i, \lambda_i\lambda_j \qquad (i, j = 1, \cdots, pr - r^2),$$

are linearly independent in $\mathfrak{F}$, but the λ_i are so small in absolute value that γ_1 and γ_2 are positive definite. This may obviously be accomplished by Theorem 56.

Let A be a multiplication of Ω. Then $\alpha\omega_1 = \omega_1 A$ where α is r-rowed, and we easily obtain

$$A_1\pi - \pi A_4 = A_2 - \pi A_3\pi, \tag{253}$$

where $A_1, \cdots, A_4$ have elements in $\mathfrak{F}$. As in our earlier proofs this implies that

$$\sum_{j=1}^{r} A_{ij}\pi_{jk} - \sum_{s=1}^{p-r} \pi_{is}B_{sk} = c_{ij} - \sum_{j,t} \pi_{ij}d_{jt}\pi_{tk} \tag{254}$$

$$(i = 1, \cdots, r;\ k = 1, \cdots, p - r),$$

whence $A_2 = A_3 = 0$. Since $r > 1$ we may take $j \neq i$ and have $a_{ij} = 0$ for $i \neq j$, $a_{ii}\pi_{jk} = \sum_s \pi_{is}\, b_{sk}$ so that $b_{sk} = 0$ for $s \neq k$ and $a_{ii} = b_{kk} = a$ in $\mathfrak{F}$. Then $A = aI_p$ as desired and Ω is a pure Omega matrix over $\mathfrak{F}$ with multiplication algebra $\mathfrak{F}$.

Suppose that R_Ω is not a central Weyl matrix. By Theorem 45 we have $\alpha\omega_1 = \bar{\omega}_2 A$ and hence $\alpha = (-\bar{\pi}'A_1 + A_2)$, $(-\bar{\pi}'A_1 - A_2)\pi = -\bar{\pi}'A_3 - A_4$. As above we immediately have $A_1 = A_4 = 0$ and

$$\sum_{j=1}^{r} a_{ij}\pi_{jk} + \bar{\pi}_{ji}b_{jk} = 0 \qquad (i = 1, \cdots, p - r;\ k = 1, \cdots, r).$$

Then $a_{kj}\pi_{jk} + \pi_{jk}b_{jk} = 0$ and $a_{kj} = -b_{jk}$. If $k \neq i$ then π_{jk} is linearly independent of π_{ji} and hence $a_{ij} = b_{jk} = 0$ for $i \neq k$. But then $a_{ij} = b_{jk} = -a_{kj} = 0$ and hence $a_{ij} = b_{jk} = 0$ for all i, j, k. Thus $A = 0$ a contradiction. Hence R_Ω is a central Weyl matrix.

Suppose that Ω_1 is a new Weyl matrix of the same form as Ω but with π_1 chosen so that the necessary products of its elements are linearly independent in the field obtained by adjoining the elements of Ω to $\mathfrak{F}$. Then $\alpha\omega_1 = \omega_{11}A$ gives $(A_1 + \pi_1 A_3)\pi = A_2 + \pi_1 A_4$ and it is easily seen that $A = 0$. Similarly Ω_1 is not isomorphic to Ω^U. Thus R_{Ω_1} and R_Ω are not associated. By an obvious induction we have Theorem 67.

Let finally $\mathfrak{F}$ be not real, $\mathfrak{F} = \mathfrak{F}_0(\rho)$. We may take $C_0 = \rho C$ instead of iC so that C_0 has elements in $\mathfrak{F}$. As before $C_0 = AE_r\bar{A}'$ where A has elements in a field obtained by the adjunction of a finite number of real square roots to $\mathfrak{F}$. Thus we may take $C_0 = E_r$ with no loss of generality and then take Ω of the form (247). But now we assume that $\pi = \tau + \sigma\rho$, $\sigma = (\sigma_{ij})$, $\tau = (\tau_{ij})$ are real matrices,

$$\mu_{i(p-r)+j} = \tau_{ij}, \qquad \nu_{i(p-r)+j} = \sigma_{ij}, \tag{255}$$

and that $h = r(p - r)$

$$1,\ \mu_k,\ \mu_k,\ \mu_s \qquad (k, s = 1, \cdots, h), \tag{256}$$

are linearly independent in $\mathfrak{F}$, while

$$1,\ \nu_k,\ \nu_k\nu_s \qquad (k, s = 1, \cdots, h), \tag{257}$$

are linearly independent in $\mathfrak{F}(\mu_1, \cdots, \mu_h)$. Then the quantities $\lambda_k = \mu_k + \rho\nu_k$ have the property that

$$1, \lambda_k, \bar{\lambda}_k, \lambda_k\lambda_s, \lambda_k\bar{\lambda}_s, \bar{\lambda}_k\bar{\lambda}_s \qquad (k, s = 1, \cdots, h), \tag{258}$$

are linearly independent in $\mathfrak{F}$. As before R_Ω is a central Weyl matrix over $\mathfrak{F}$ with $\mathfrak{F}$ as multiplication algebra while $(R_\Omega)^2 = i_0^2 I_p$, $R_\Omega = i_0\Omega^{-1}E_r\Omega$.

The Weyl matrix

$$\bar{R}_\Omega = \bar{i}_0^{-1}\bar{\Omega}^{-1}E_r\bar{\Omega} = R_{\bar{\Omega}}, \text{ or } \bar{R} = R_{\bar{\Omega}^U}, \tag{259}$$

according as $i_0 = 1$ or $i_0 = -1$. We have shown that if

$$\Omega_0 = \begin{pmatrix} \omega_{01} \\ \bar{\omega}_{02} \end{pmatrix}, \qquad \Omega_0^U = \begin{pmatrix} \bar{\omega}_{02} \\ \omega_{01} \end{pmatrix}, \tag{260}$$

then $AR_\Omega A^{-1} = R_{\Omega_0}$ if and only if Ω and Ω_0 *are isomorphic by* A, that is

$$\alpha_1\omega_1 = \omega_{01}A, \qquad \alpha_2\bar{\omega}_2 = \bar{\omega}_{02}A. \tag{261}$$

We have also proved that when R_Ω is not isomorphic to R_{Ω_0} but is associated with R_{Ω_0} then R_Ω is isomorphic to $R_{\Omega_0^U}$. Hence if Ω is not isomorphic to $\bar{\Omega}$ or $\bar{\Omega}^U$ the matrix R_Ω will not be associted with $\bar{R}_\Omega$. Thus it is sufficient to prove that either $\alpha\omega_1 = \bar{\omega}_1A$ or $\alpha\omega_1 = \omega_2A$ if and only if $A = 0$. A trivial repetition of our above argument gives this result and an obvious construction of further matrices $\Omega_2, \cdots, \Omega_m$ proves

THEOREM 68. *Let $\mathfrak{F} = \mathfrak{F}_0(\rho)$, $\bar{\rho} = -\rho$, m and $p > 2$ be positive integers, $C_i = \pm \bar{C}_i'$ be non-singular matrices, and assume $i_0 = 1$, i such that $C_{0i} = i_0C_i$ is Hermitian of index r. Then there exist central Weyl matrices $R_1, \cdots, R_m$ with principal matrices C_i respectively, multiplication algebras $\mathfrak{F}$, $R_i^2 = i_0^2I_p$, and R_i is not associated with $\bar{R}_i, R_j, \bar{R}_j$ for $i \neq j$; $i, j = 1, \cdots, m$.*

The considerations of sections 4 and 5 combined with Theorems 66, 67, 68 prove the existence of Weyl matrices R_Ω with a given algebra $\mathfrak{A}$ of Theorem 27 as multiplication algebra except when R is real and $\mathfrak{A} = Q \times \mathfrak{A}_1$ over a real field $\mathfrak{F}$. For this case we let

$$C = \epsilon\bar{C}', \qquad \epsilon = \pm 1, \qquad Y\overline{CY}' = C, \qquad Y\bar{Y} = -Ip, \tag{262}$$

where C and Y are non-singular square matrices with elements in $\mathfrak{F}(i)$ and C is given while Y is at our choice. We then wish to construct a matrix R such that $R = R_\Omega$ has principal matrix C and $\bar{R} = Y^{-1}RY$. We have also proved that the Hermitian matrix $C_0 = i_0C$ may be taken to have the form

$$AC_0\bar{A}' = \begin{bmatrix} e_1 & 0 & 0 & 0 \\ 0 & e_1 & 0 & 0 \\ 0 & 0 & -e_2 & 0 \\ 0 & 0 & 0 & -e^2 \end{bmatrix}, \qquad p = 2\beta + 2\gamma, \tag{263}$$

where e_1 and e_2 are diagonal matrices of positive elements and e_1 has β rows. Thus we are not attempting to construct the most general R_Ω but *merely a convenient* R_Ω in order to complete our existence theory.

If $Y_0 = AY\bar{A}^{-1}$ then $Y_0\bar{Y}_0 = -I_p$, $Y_0\overline{AC\bar{A}'\bar{Y}_0'} = AC\bar{A}'$ and the matrix $R_0 = ARA^{-1}$ has the property $Y_0^{-1}R_0Y_0 = \bar{R}_0$. Then R_0 is isomorphic to R and we may assume that

$$(264) \qquad i_0C = C_0 = \begin{bmatrix} e_1 & 0 & 0 & 0 \\ 0 & e_1 & 0 & 0 \\ 0 & 0 & -e_2 & 0 \\ 0 & 0 & 0 & -e_2 \end{bmatrix},$$

without loss of generality.

Assume first that $C = C_0$ is Hermitian so that the matrix Y, given by

$$(265) \qquad Y = \begin{pmatrix} \eta_1 & 0 \\ 0 & \eta_2 \end{pmatrix}, \qquad \eta_1 = \begin{pmatrix} 0 & -I_\beta \\ I_\beta & 0 \end{pmatrix}, \qquad \eta_2 = \begin{pmatrix} 0 & -I_\gamma \\ I_\gamma & 0 \end{pmatrix},$$

is commutative with C and has the properties

$$Y^2 = Y\bar{Y} = -I_p, \qquad Y\overline{CY}' = YCY' = YCY^{-1} = C.$$

Also the matrix

$$(266) \qquad B = \begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & -a_2 \end{bmatrix}, \qquad a_1^2 = e_1, \qquad a_2^2 = e_2,$$

is a diagonal matrix with elements in a finite real extension $\mathfrak{F}_1$ of $\mathfrak{F}$ and is commutative with $Y, C = BE_{2\beta}B'$. Then BRB^{-1} is isomorphic to R in $\mathfrak{F}_1$, $R_1 = BRB^{-1}$ has $E_{2\beta}$ as principal matrix,

$$Y^{-1}R_1Y = BY^{-1}RYB^{-1} = B\bar{R}B^{-1} = \bar{R}_1, \qquad Y\bar{E}_{2\beta}\,\bar{Y}_1 = YE_{2\beta}\,Y^{-1} = E_{2\beta}.$$

The matrix R must have the property $R^2 = I_p$ and obviously $R_1^2 = I_p$. If R_1 as only scalar multiplications with elements in $\mathfrak{F}_1$ then R obviously has the same property and hence the $\mathfrak{F}$-algebra of R is $\mathfrak{F}$.

We may thus take $C = E_{2\beta}$ without loss of generality and write

$$R_\Omega = \Omega^{-1}E_{2\beta}\Omega,$$

where Ω is given by (247). Then (261) gives

$$(267) \qquad \alpha_1\bar{\omega}_1 = \omega_1Y, \qquad \alpha_2\omega_2 = \bar{\omega}_2Y,$$

and (267) is equivalent to the single condition

$$\eta_1\bar{\pi} = \pi\eta_2. \tag{268}$$

We write

$$\pi = \begin{pmatrix} \pi_1 & \pi_2 \\ \pi_3 & \pi_4 \end{pmatrix}, \tag{269}$$

where $\pi_1, \cdots, \pi_4$ each have β rows and γ columns and (268) is equivalent to

$$\pi_3 = -\bar{\pi}_2, \qquad \pi_4 = \bar{\pi}_1. \tag{270}$$

We use the notation of (251) and use Lemma 2 to make (252) linearly independent in $\mathfrak{F}(i)$. As in our above proof of Theorem 68 the equation (253) is impossible unless A_1 and A_4 are equal scalar multiples of identity matrices and A_2 and A_3 are zero matrices. Thus R_Ω has only scalar multiplications. If $(\bar{\pi}'A_1 + A_2)\pi = \pi'A_3 + A_4$ then A_1 and A_4 are zero matrices and

$$\begin{gathered} A_2\pi = \bar{\pi}'A_3, \qquad \bar{\pi}' = \eta_2\pi'\eta_1^{-1}, \qquad A_{20}\pi = \pi'A_{30}, \\ \sum_{j=1}^{2\beta} a_{ij}\pi_{jk} - \sum_{j=1}^{2\beta} b_{kj}\pi_{ji}. \qquad (i, k = 1, \cdots, 2\gamma). \end{gathered} \tag{271}$$

The linear independence of (253) in $\mathfrak{F}(i)$ implies that $A_2 = A_3 = 0$ and R_Ω is a central Weyl matrix.

We next let $C = -\bar{C}'$, $C_0 = iC$,

$$R_\Omega = i^{-1}\Omega^{-1}E_{2\beta}\Omega = i^{-1}R_0, \tag{272}$$

whence

$$Y\bar{C}_0\bar{Y}' = -C_0, \qquad Y^{-1}R_0Y = -\bar{R}_0. \tag{273}$$

We have seen that necessarily $\beta = \gamma$ and $-\bar{R}_0 = (\bar{\Omega}^U)^{-1}E_{2\beta}\bar{\Omega}^U = Y^{-1}R_0Y$ if and only if

$$\alpha_1\omega_2 = \omega_1Y, \qquad \alpha_2\bar{\omega}_1 = \bar{\omega}_2Y. \tag{274}$$

We may take $Y^2 = -I_p$, $Y' = -Y$ where Y is a real matrix but C_0 is not in its canonical form (264). The reduction of C_0 to its canonical form (264) may be accomplished by a unitary transformation $A = (\bar{A}')^{-1}$ and this replaces Y by $Y_0 = AY\bar{A}^{-1}$, $Y_0\bar{Y}_0' = AY\bar{A}^{-1}A'^{-1}Y^{-1}\bar{A}' = I_p$ since $\bar{Y}' = Y' = -Y = Y^{-1}$, $\bar{A}'A = I_p$, $A'\bar{A} = I_p$, $\bar{A}^{-1}A'^{-1} = I_p$. Thus we may assume that the matrix C_0 of (264) has the property $YC_0\bar{Y}' = YC_0Y^{-1} = -C_0$. But then the characteristic determinants of the diagonal matrices e_1 and e_2 are identical and C_0 may be carried into

$$\begin{pmatrix} e_1 & & & \\ & e_1 & & \\ & & -e_1 & \\ & & & -e_1 \end{pmatrix} \tag{275}$$

by a unitary transformation. Hence we may assume that C_0 has the form (275).

We now take

$$Y = \begin{pmatrix} 0 & I_{2\beta} \\ -I_{2\beta} & 0 \end{pmatrix}, \tag{276}$$

and again have Y commutative with

$$B = \begin{bmatrix} b_1 & 0 & 0 & 0 \\ 0 & b_1 & 0 & 0 \\ 0 & 0 & b_1 & 0 \\ 0 & 0 & 0 & b_1 \end{bmatrix}. \tag{277}$$

As before we may take $C_0 = E_{2\beta}$ without loss of generality and we now take

$$\Omega = \begin{pmatrix} w_1 \\ \bar{w}_2 \end{pmatrix}, \qquad \omega_2 = \omega_1 Y, \tag{278}$$

so that (274) are satisfied. Moreover if π is a non-singular skew-symmetric matrix whose distinct elements λ_j have the property that

$$1,\ \lambda_j,\ \bar{\lambda}_j,\ \lambda_j\lambda_k,\ \lambda_j\bar{\lambda}_k, \tag{279}$$

are linearly independent in $\mathfrak{F}(i)$ but sufficiently small in absolute value so that $I_2 - \pi\bar{\pi}'$ is positive definite, then

$$\omega_1 E_{2\beta}\omega_2' = (I_{2\beta},\ \pi) \begin{pmatrix} 0 & I_{2\beta} \\ I_{2\beta} & 0 \end{pmatrix} \begin{pmatrix} I_{2\beta} \\ \pi' \end{pmatrix} = \pi + \pi' = 0, \tag{280}$$

$$\gamma = \omega_1 E_{2\beta}\omega_1' = I_{2\beta} - \pi\bar{\pi}', \tag{281}$$

$$\bar{\gamma} = -\ \bar{\omega}_2 E_{2\beta}\omega_2' = -\ (\bar{\pi},\ I_{2\beta}) \begin{pmatrix} I_{2\beta} & 0 \\ 0 & -I_{2\beta} \end{pmatrix} \begin{pmatrix} \pi' \\ -I_{2\beta} \end{pmatrix} = I_2 - \bar{\pi}\pi', \tag{282}$$

and R_Ω is a Weyl matrix with principal matrix C. I have proved elsewhere[68] that $\alpha\omega_1 = \omega_1 A$ if and only if A is a scalar matrix so that R_Ω has only scalar multiplications. If R_Ω were not a central Weyl matrix we would have $\alpha\omega_1 = \bar{\omega}_2 A$ for A not zero and thus $\alpha\omega_1 = \bar{\omega}_1 A$ for A not zero since $\bar{\omega}_2 = \bar{\omega}_1 Y$. Thus $\alpha = A_1 + \pi A_2$ and $A_1\pi + \pi A_2\pi\ iA_3 + \pi A_4$. The linear independence of (279) implies immediately that $A_2 = A_3 = 0$, $A_1\pi = \pi\ A_4$. We have chosen π so that its elements are linearly independent of the elements of $\bar{\pi}$ in the field containing the elements of A_1 and A_4. Hence $A_1 = A_4 = 0$.

The method of proof by which we obtained Theorem 62 will now give non-associated matrices R_{Ω_i} and the argument of Sections 4 and 5 now proves the

---

[68] Albert (4).

existence of a Weyl matrix R_Ω over $\mathfrak{F}$ with $\mathfrak{D}$ as multiplication algebra and such that $R_\Omega^2 = \epsilon I_p$, $C = \epsilon C'$, $\epsilon = \pm 1$. But we may obtain a more important further result.

Let $\mathfrak{K}_0 = \mathfrak{F}(S)$ be the T-symmetric part of the centrum of $\mathfrak{D}$ and let $\delta = \delta(S)$ in $\mathfrak{K}_0$ have the property that δ is total positive when $C = -C'$ and δ is total negative when $C = C'$. Then $\mathfrak{K}_0$ has conjugate fields $\mathfrak{F}(\sigma_j)$ and $\delta_j = \delta(\sigma_j)$,

$$(283) \qquad -\delta_j\epsilon > 0\,, \qquad \gamma_j = (-\delta_j\epsilon)^{\frac{1}{2}} \qquad (j = 1, \cdots, t)\,,$$

is positive. We now construct a set of t real central Weyl matrices R_{j^0} over $\mathfrak{F}_j = (\sigma_j, \gamma_j)$ such that R_{j^0} has $\mathfrak{D}_j$ over $\mathfrak{F}_j$ as multiplication algebra, principal matrix C_j and R_{i^0} is not associated with R_{j^0} in $\mathfrak{F}(\sigma_1, \cdots, \sigma_t; \gamma_1, \cdots, \gamma_t)$ for $i \neq j$. We also let $R_{j^0}^2 = \epsilon I_\pi$ so that if $R_j = \gamma_j R_{j^0}$ then R_j is a positive multiple of $R_j{}^0$ by quantity of $\mathfrak{F}_j$ and $R_j^2 = -\delta_j I_\pi$. Moreover R_j is a real central Weyl matrix over $\mathfrak{F}(\sigma_j)$ and has $\mathfrak{D}_j$ over $\mathfrak{F}(\sigma_j)$ as multiplication algebra. Then the corresponding matrix R of (174) is a real central Weyl matrix over $\mathfrak{F}$ with the property $R^2 = -\delta$ in $\mathfrak{K}_0$ and with $\mathfrak{D}$ as multiplication algebra.

Conversely let $R^2 = -\delta$ have C as principal matrix, $C = \epsilon\, C'$. Then we adjoin $\mathfrak{K}_0$ and have $R_j^2 = -\delta_j I_\pi$, $R_{j^0}^2 = \epsilon_{0j} I_\pi$ where ϵ_{0j} is the product of the sign of δ_j by -1. But $C_j' = \epsilon\, C_j$ and Theorem 42 states that $R_{j^0}^2 = \epsilon I_\pi$, δ_j is positive if $C' = -C$, δ_j is negative if $C' = C$. We have proved

THEOREM 69. *Let $\mathfrak{D}$ be an algebra of Theorems* 27–30 *over a real field $\mathfrak{F}$ and let δ in the T-symmetric sub-field $\mathfrak{K}_0$ of the centrum of $\mathfrak{D}$ be either total positive or total negative. Then there exists a real central Weyl matrix R over $\mathfrak{F}$ with $\mathfrak{D}$ as multiplication algebra and $R^2 = -\delta$. Conversely $R^2 = -\delta$ and R has $C = \epsilon\, C'$ as principal matrix only when δ is total positive if $C = -C'$, δ is total negative if $C = C'$.*

12. **Pure real Riemann matrices with $\mathfrak{A} = \mathfrak{D}_0$.** Let $\mathfrak{D}_0$ be any involutorial division algebra over a real field $\mathfrak{F}$ and satisfying the conditions of Theorem 28. Theorem 65 states that there exists a real central Weyl matrix R not associated with R^{-1} and such that $\mathfrak{D}$ is the multiplication algebra of R. From Theorem 52 we conclude that the multiplication algebra of $\omega = (R, iI_p)$ is $\mathfrak{D}_0$ equivalent to $\mathfrak{D}$ and have proved

THEOREM 70. *There exist pure real Riemann matrices with any given division algebra $\mathfrak{D} = \mathfrak{D}_0$ as multiplication algebra if and only if $\mathfrak{D}$ is an algebra of Theorems* 27–30.

13. **The first case $\mathfrak{A} \neq \mathfrak{D}_0$.** Consider a pure real Riemann matrix $\omega = (R, iI_p)$ over a real field $\mathfrak{F}$ and let $\mathfrak{D}$ be the multiplication algebra of R, $\mathfrak{D}_0$ the equivalent sub-algebra of the multiplication algebra $\mathfrak{A}$ of ω. Assume that R is associated with R^{-1}. By Theorem 52 we have $\mathfrak{A} \neq \mathfrak{D}_0$.

Consider the case where R is a matrix of Theorem 39. By Theorem 51 and 39 we may choose R so that

$$R^2 = -\delta$$

where $\delta = \delta^T$ is in the T-symmetric part $\mathfrak{K}_0$ or $\mathfrak{D}$. Moreover

$$(284) \qquad \mathfrak{A} = \mathfrak{D} \times (1, g), \qquad g = \begin{pmatrix} 0 & I_p \\ \delta & 0 \end{pmatrix}, \quad g^2 = \delta .$$

If C is a principal matrix of R then

$$(285) \qquad \begin{pmatrix} 0 & C \\ -C' & 0 \end{pmatrix}$$

is a principal matrix of ω and we have $C' = \epsilon C$, $C\delta' C^{-1} = \delta^T = \delta$,

$$(286) \qquad g^T = \begin{pmatrix} 0 & C \\ -\epsilon C & 0 \end{pmatrix} \begin{pmatrix} 0 & \epsilon' \\ I_p & 0 \end{pmatrix} \begin{pmatrix} 0 & -\epsilon C^{-1} \\ C^{-1} & 0 \end{pmatrix} = -\epsilon g,$$

and

$$(287) \quad (a_A)^T = \begin{pmatrix} 0 & C \\ -\epsilon C & 0 \end{pmatrix} \begin{pmatrix} A' & 0 \\ 0 & A' \end{pmatrix} \begin{pmatrix} 0 & -\epsilon C^{-1} \\ C^{-1} & 0 \end{pmatrix} = \begin{pmatrix} CA'C^{-1} & 0 \\ 0 & CA'C^{-1} \end{pmatrix} = \begin{pmatrix} A^T & 0 \\ 0 & A^T \end{pmatrix}.$$

The above treatment completely determines the structure of $\mathfrak{A}$ and its involution T in terms of δ and the structure of $\mathfrak{D}$ and its involution T. If $C = C'$ then $g^T = -g$ so that the characteristic roots of δ must be all negative. If $C = -C'$ then they must be all positive since then $g^T = g$. This gives a new proof of the condition on δ of Theorem 69. We have also the following restatement of Theorem 69.

THEOREM 71. *Let $\mathfrak{D}$ over a real field $\mathfrak{F}$ be any division algebra of Theorems* 27–30, *and δ be a total positive or total negative quantity of $\mathfrak{K}_0$ such that the algebra $\mathfrak{A}$ of* (278) *is a division algebra. Then there exist pure real Riemann matrices with $\mathfrak{A}$ as multiplication algebra.*

14. **The second case $\mathfrak{A} \neq \mathfrak{D}_0$.** Let ω be a pure real Riemann matrix not of the type of sections 12, 13, and let Σ be the centrum of the multiplication algebra $\mathfrak{A}$ of ω. By Theorem 52 and the proof of Theorem 41 the algebra $\mathfrak{A}$ contains a quantity $u = \pm u^T$ such that $\delta = u^2$ is in Σ. Moreover $\delta = \delta^T$ is obviously either total positive or total negative and $\mathfrak{A}$ is an algebra of Theorems 27–30.

Conversely let $\mathfrak{A}$ be a division algebra of Theorem 27–30 and let $\mathfrak{A}$ contain a quadratic extension $\Sigma(u)$ of its centrum such that $u^2 = \delta$ is a total positive or total negative quantity of Σ. Then the involution T of $\mathfrak{A}$ may be so chosen that $u^T = \pm u$. We shall only consider the case where $u^T = u$ so that u^2 is a total positive quantity of Σ. Moreover we may take $C = C'$.[69]

The algebra $\mathfrak{D}$ of all quantities A of $\mathfrak{A}$ such that $Au = uA$ is a normal division algebra over its centrum $\mathfrak{K} = \Sigma(u)$. If $Au = uA$ then $uA^T = A^T u$ and A^T is in $\mathfrak{D}$, $\mathfrak{D}$ is T-involutorial. There exists a quantity g in $\mathfrak{A}$ such that $gu = -ug$,

[69] As in Theorem 51.

$g^2 = y$ is in $\mathfrak{D}$. But also $g^T u = -ug^T$ and we may select g so that $g^T = \pm g$. We consider a p-rowed representation of $\mathfrak{A}$ by matrices with elements in $\mathfrak{F}$ and let

$$a \leftrightarrow A\,, \qquad u \leftrightarrow U\,, \qquad g \leftrightarrow G\,, \tag{288}$$

for every a of $\mathfrak{A}$. Then $\mathfrak{A}$ has the $2p$-rowed representation

$$a \leftrightarrow a_A = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}, \qquad g \leftrightarrow \begin{pmatrix} 0 & -G \\ -G & 0 \end{pmatrix}, \qquad H = -G\,. \tag{289}$$

We now prove the existence theorem.

THEOREM 72. *There exist real Riemann matrices with the above algebra $\mathfrak{A} = \mathfrak{D} + \mathfrak{D}\,g$ as multiplication algebra.*

For the T-symmetric part of Σ is a field Σ_0 which we may adjoin in our usual manner. Hence we may take $\Sigma_0 = \mathfrak{F}$, $u^2 = \alpha > 0$ in $\mathfrak{F}$ without loss of generality. Then we let $p = 2\pi$,

$$V_U = \begin{pmatrix} I_\pi & \alpha^{\frac{1}{2}} I_\pi \\ I_\pi & -\alpha^{\frac{1}{2}} I_\pi \end{pmatrix}, \qquad V_U U V_U^{-1} = \begin{pmatrix} \alpha^{\frac{1}{2}} I_\pi & 0 \\ 0 & -\alpha^{\frac{1}{2}} I_\pi \end{pmatrix}, \tag{290}$$

and $GU = -UG$ gives

$$G_0 = V_U G V_U^{-1} = \begin{pmatrix} 0 & G(\alpha^{\frac{1}{2}}) \\ G(-\alpha^{\frac{1}{2}}) & 0 \end{pmatrix}, \qquad V_U C V_{U'} = \begin{pmatrix} C(\alpha^{\frac{1}{2}}) & 0 \\ 0 & C(-\alpha^{\frac{1}{2}}) \end{pmatrix}. \tag{291}$$

Let R_1 be a real central Weyl matrix over $\mathfrak{F}(\alpha^{\frac{1}{2}})$ with principal matrix $C(\alpha^{\frac{1}{2}})$ and $\mathfrak{D}$ over $\mathfrak{F}(\alpha^{\frac{1}{2}})$ as multiplication algebra, and assume that R_1 is not associated with R_1^{-1}. Such a matrix exists by Theorem 64.

Write $G_1 = G(\alpha^{\frac{1}{2}})$, $G_2 = G(-\alpha^{\frac{1}{2}})$ and take

$$R_2 = -G_1^{-1} R_1^{-1} G_1\,, \tag{292}$$

a matrix not associated with R_1 since R_2 is associated with R_1^{-1}. Then

$$G_0^2 = \begin{pmatrix} G_1 G_2 & 0 \\ 0 & G_2 G_1 \end{pmatrix} = V_U G^2 V_U^{-1}\,, \tag{293}$$

so that $G_1 G_2$ is in $\mathfrak{D}$ over $\mathfrak{F}(\alpha^{\frac{1}{2}})$ and is commutative with R_1, R_1^{-1}. But (292) implies that $R_2 = -G_2 R_1^{-1} G_2^{-1}$ and thus

$$R_1 G_1 R_2 = -G_1\,, \qquad R_2 G_2 R_1 = -G_2 \tag{294}$$

from which

$$V_U R V_U^{-1} = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}, \qquad RGR = -G = H\,. \tag{295}$$

The matrix R_1 has principal matrix $C_1 = C_{1'}$ and Theorem 37 states that C_1 is also a principal matrix of R_1^{-1}, $G_2C_1G_{2'}$ is a principal matrix of R_2. Also $CG'C^{-1} = \beta\, G$ implies that $C_1G_2C_2^{-1} = \beta\, G_1$, $(\beta G_2G_2)C_2 = G_2C_1G_{2'}$. The quantity $g = \beta g^T$ has the property that g^2 is a symmetric quantity of $\mathfrak{D}$ which is total positive or total negative according as $\beta = 1$ or -1. Hence βg^2 is total positive, βG_2G_1 is total positive and commutative with R_2, C_2 is a principal matrix of R_2. Then R is a real Weyl matrix over $\mathfrak{F}$ and has $\mathfrak{D}$ over its centrum $\mathfrak{F}(u)$ as multiplication algebra and the property $-G = RGR$.

We not let $\omega = (R, iI_p)$ so that

$$A\omega = \omega \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}, \qquad (A \text{ in } \mathfrak{D}),$$

while

$$iRG\,\omega = \omega \begin{pmatrix} 0 & -G \\ -G & 0 \end{pmatrix}.$$

Thus ω has $\mathfrak{A}$ as multiplication algebra and we have constructed pure real Riemann matrices of the three possible types.

VIII. Table of Literature

A. A. Albert: (1) *On the structure of pure Riemann matrices with non-commutative multiplication algebras*, Palermo Rendiconti, vol. 55 (1931), pp. 57–115; (2) *The structure of matrices with any normal division algebra of multiplications*, these Annals, vol. 32 (1931), pp. 131–148; (3) *Algebras of degree 2^e and pure Riemann matrices*, these Annals, vol. 33 (1932), pp. 311–318; (4) *On the construction of Riemann matrices I*, these Annals, vol. 35 (1934), pp. 1–28; (5) *A solution of the principal problem in the theory of Riemann matrices* these Annals, vol. 35 (1934), pp. 500–515; (6) *A note on the Poincaré theorem on impure Riemann matrices*, these Annals, vol. 36 (1935), pp. 151–156; (7) *On the construction of Riemann matrices* II, these Annals, April 1935; (8) *On direct products, cyclic division algebras and pure Riemann matrices*, Transactions of the American Mathematical Society, vol. 33 (1931), pp. 219–234; (9) *On direct products*, Transactions, vol. 33 (1931), pp. 690–711; (10) *On normal simple algebras*, Transactions, vol. 34 (1932), pp. 620–625; (11) *A determination of all normal division algebras over an algebraic number field*, (with H. Hasse), Transactions, vol. 34 (1932), pp. 722–726; (12) *On the rank equation of any normal division algebra*, Bulletin of the American Mathematical Society, vol. 35 (1929), pp. 335–338; (13) *A note on an important theorem on normal division algebras*, Bulletin, vol. 36 (1930), pp. 535–540; (14) *Division algebras over an algebraic number field*, Bulletin, vol. 37 (1931), pp. 777–784; (15) *The principal matrices of a Riemann matrix*, Bulletin, vol. 40 (1934), pp. 843–846; (16) *The rank function of any simple algebra*, Proceedings of the National Academy of Sciences, vol. 15 (1929), pp. 372–376.

E. Artin: (1) *Algebraische Konstru ion reeler Körper*, Hamburg Abhandlungen, vol. 5 (1927), pp. 83–115; (2) *Eine Kennzeichnung über algebraische abgeschlossenen Zahlkörper*, Hamburg Abhandlungen as in (1), pp. 225–231 (both with O. Schreier).

R. Brauer: *Über Systeme hyperkomplexen Zahlen*, Mathematische Zeitschrift, vol. 30 (1929), pp. 70–107.

S. Cherubino: (1) *Sulle varieta abeliane reale, e sulle matrici di Riemann reali* I, Giornale di matematiche, vol. 60 (1922), pp. 65–94; (2) Same as I, vol. 61 (1923), pp. 47–68.

A. Comessatti: (1) *Fondamenti per la Geometria sopra le superficie razionali dal punto di vista reale*, Mathematische Annalen, vol. 73 (1913), pp. 1–72; (2) *Sulle varieta abeliane reali*, Annali di matematica, vol. 2 (1925), pp. 67–106; (3) Same title and journal as (2), vol. 3 (1926), pp. 27–71.

L. E. Dickson: *Algebren und ihre Zahlentheorie*, Zurich, 1926.

W. Franz: *Untersuchungen zum Hilbertschen Irreduzibilitätssatz*, Mathematische Zeitschrift, vol. 33 (1931), pp. 275–293.

W. Grünwald: *Ein allgemeines Existenztheorem für algebraische Zahlkörper*, Journal für Mathematik, vol. 169 (1933), pp. 103–107.

H. Hasse: (1) *Über 𝔓-adische Scheifkörper*, Mathematische Annalen, vol. 104 (1931), pp. 495–534; (2) *Theory of cyclic algebras over an algebraic number field*, Transactions, vol. 34 (1932), pp. 171–214; (3) *Klassenkörpertheorie*, Marburg 1932; (4) See Albert (11).

D. Hilbert: *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, Journal für Mathematik, vol. 110 (1892), pp. 104–129.

F. Klein: (1) *Über Realitätsverhältnisse bei der einem beliebigen Geschlechte*, etc., Mathematische Annalen, vol. 42 (1893), pp. 1–29; (2) *Riemann'sche Flächen*, vol. II, Göttingen, 1892.

S. Lefschetz: (1) *On certain numerical invariants of algebraic varieties with application to abelian varieties*, Transactions, vol. 22 (1921), pp. 827–482; (2) *On the real folds of abelian varieties*, Proceedings of the National Academy of Sciences, vol. 5 (1919), pp. 103–105; (3) *Real hypersurfaces contained in abelian varieties*, same as (2), pp. 296–298; (4) *Selected Topics on Algebraic Geometry*, Bulletin of the National Research Council, 63, 1928, pp. 310–394.

C. Rosati: (1) *Sulle corrispondenze fra i punti di una curva algebrica*, etc., Annali di matematica, vol. 25 (1916), pp. 1–32; (2) *Sulle corrispondenze algebriche fra i punti di due curve algebriche*, Ann. di Mat., vol. 28 (1919), pp. 35–61; (3) Sulle matrici di Riemann, Palermo Rendiconti, vol. 53 (1929), pp. 79–134.

O. Schreier: See Artin (1), (2).

G. Scorza: (1) *Corpi numerici e Algebra*, 192[illegible]; (2) *Intorno alla teoria generale delle matrici di Riemann*, Palermo Rendiconti, vol. 41 (1916), pp. 263–380; (3) *Le algebre di ordine qualunque e le matrici di Riemann*, Palermo Rendiconti, vol. 45 (1921), pp. 1–204.

Van der Waerden: *Moderne Algebra*, Berlin, 1930.

J. H. M. Wedderburn: (1) *On hypercomplex numbers*, Proceedings of the

London Mathematical Society, vol. 6 (1907), pp. 77–118; (2) *Note on hypercomplex numbers*, Proceedings of the Edinburgh Mathematical Society, vol. 25 (1906–7), pp. 1–3; (3) *A theorem on simple algebras*, Bulletin, vol. 31 (1925), pp. 11–13; (4) *Lectures on matrices*, American Mathematical Society Colloquium Publications, New York, 1934.

H. Weyl: (1) *Idee der Riemannschen Fläche*, 2te Auflage, Leipzig, 1923; (2) *On generalized Riemann matrices*, these Annals, vol. 35 (1934), pp. 714–729.

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILLINOIS.

ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

NON-RIEMANNIAN SUBSPACES

BY A. W. TUCKER

(Received May 24, 1935)

This paper[1] treats in formal fashion some general aspects of the differential geometry of subspaces. The setting is non-Riemannian[2] except at the end where the Riemannian case appears as a specialization. We develop the idea of osculating subspace and obtain general formulas of the Frenet and Gauss-Codazzi type. These formulas (which will be found labeled F1, GC1, F2, etc.) arise in an interesting and suggestive manner from appropriate decompositions of our principal space into sets of independent subspaces.

I. FOUNDATIONS

In dealing with a *space* in modern differential geometry one has to do with a system of *local spaces* defined over an *underlying space* and a *displacement* which maps neighboring local spaces on to one another.[3] For example, the underlying space of an n-dimensional Riemannian space is a manifold of n dimensions, the local spaces are the n-dimensional spaces of differentials "tangent" to the underlying space, and the displacement is that determined by the fundamental metric. For our work we take an m-dimensional space V whose underlying space is an n-dimensional manifold X, whose local spaces are m-dimensional vector spaces, and whose displacement is determined by a *linear connection* L.

By a vector of V we mean a vector-field defined over the underlying space X, the local vectors of the field being elements of the local spaces of V. By a subspace V_0 of our principal space V we mean a space whose underlying space is X, whose local spaces are linear subspaces of the local spaces of V, and whose displacement is determined by a linear connection L_0^0. The dimension of V_0 is understood to be a constant m_0; should our operations lead to subspaces which degenerate (i.e. lower their dimensions) at special points x of the underlying space X we confine our attention to a region of the underlying space which excludes these singular points. It is assumed of course that X is a regular[3] manifold and that the functions with which we deal are regular on X.

1. Basic notation. We begin with the vector algebra in our local spaces, for in this algebra our notation has its roots.

---

[1] Developed in part while the author was a National Research Fellow.

[2] In the sense of Eisenhart, *Non-Riemannian Geometry* (Am. Math. Soc. Coll. Publ., 1927).

[3] See Veblen and Whitehead, *The foundations of differential geometry*, (Cambridge Tract, 1932).

By a *basis* for V we mean a set $\{v_a\}$ of m linearly independent vectors $v_1, v_2, \cdots, v_m$, in terms of which each vector of V has a unique linear expression; the coefficients in the unique expression are called the *components* of the vector with respect to the basis. Let $\{v_{a'}\}$ be a second basis for V. Then, since the vectors of one basis are uniquely expressible in terms of the vectors of another basis, we have

$$v_{b'} = v_a v^a_{b'} = v_{a'} v^{a'}_{b'} \qquad \text{and} \qquad v_b = v_a v^a_b = v_{a'} v^{a'}_b ,$$

where

$$v^a_b = v^a_{b'} v^{b'}_b = v^a_{a'} v^{a'}_b = v^a_{a'} v^{a'}_{b'} v^{b'}_b .$$[4]

$v^a_{b'}$ are the components of the basis vector $v_{b'}$ with respect to the basis $\{v_a\}$, and $v^{a'}_{b'}$ (= the Kronecker delta $\delta^{a'}_{b'}$) are those of the same vector with respect to $\{v_{a'}\}$; $v^a_b (= \delta^a_b)$ are the components of the basis vector v_b with respect to $\{v_a\}$, and $v^{a'}_b$ are those with respect to $\{v_{a'}\}$. But $v^a_{b'}, v^{a'}_{b'}, v^a_b, v^{a'}_b$ have also another important interpretation as the last display of equations shows; they are the components of a mixed tensor. Abstracting indices we denote this tensor by v.

The discussion of the last paragraph carries over at once to a subspace V_0 of our principal space V. We have only to add a subzero to all the indices. Thus $\{v_{a_0}\}$, $\{v_{a'_0}\}$ denote bases for V_0. In particular it is natural to denote the tensor abstracted from $v^{a_0}_{b'_0}$, etc., by v^0_0.

Since V_0 is a subspace of V we have

$$v_{a_0} = v_a v^a_{a_0} .$$

$v^a_{a_0}$ are the components of the basis vector v_{a_0} with respect to the basis $\{v_a\}$. Using other combinations of bases from V_0 and V we could get sets of components $v^{a'}_{a_0}, v^a_{a'_0}, v^{a'}_{a'_0}$, where

$$v^a_{a_0} = v^a_{a'} v^{a'}_{a_0} = v^a_{a'_0} v^{a'_0}_{a_0} = v^a_{a'} v^{a'}_{a'_0} v^{a'_0}_{a_0} .$$

These are sets of components of a tensor which through abstraction we denote by v_0. v_0 is an example of a tensor referred in part to one space (V) and in part to another (V_0). We shall have much to do with such "hybrid" tensors.

The notation for other subspaces of V to be introduced (V_1, V_2, etc.) will be like that for V_0; the subzero will be replaced by another subindex (1, 2, etc.).

2. Absolute differentiation. We now pass to differential geometry proper. We define operations of differentiation founded on the underlying space X and the linear connections L, L^0_0.

---

[4] a, b, etc. form one set of interchangeable indices; a', b', etc. form another set. This means, for example, that $\{v_a\}$ and $\{v_b\}$ denote the same basis.

The summation convention is understood throughout.

If x^{i^1} and x^{i^2} are the coördinates of two overlapping systems in the underlying space X we can regard

$$dx^{i^1} \quad \text{and} \quad dx^{i^2} = \frac{\partial x^{i^2}}{\partial x^{i^1}} dx^{i^1}$$

as the components of a vector, which we denote by dx, with reference to two bases, which we denote by

$$\{v_{i^1}\} = \left\{\frac{\partial x}{\partial x^{i^1}}\right\} \quad \text{and} \quad \{v_{i^2}\} = \left\{\frac{\partial x}{\partial x^{i^2}}\right\}.$$

The space of the vectors dx is a vector space of n dimensions, which we denote by V_x; it is called the "tangent space" of the underlying space X.[5] Let $\{v_i\}$ be an arbitrary basis for V_x. Then

$$v_i = \frac{\partial x}{\partial x^{i^s}} v_i^{i^s} \quad \text{and} \quad \frac{\partial x}{\partial x^{i^s}} = v_i v^i_{i^s} \qquad (s = 1, 2).$$

If x^i exist so that $v^i_{i^s} = \partial x^i / \partial x^{i^s}$ we call $\{v_i\}$ a *holonomic* basis, and we write $\{v_i\} = \{\partial x / \partial x^i\}$. The general basis $\{v_i\}$ however is non-holonomic.

We use a comma to denote the "directional" differentiation

$$Q_{,i} = \left(\frac{\partial}{\partial x^{i^s}} Q\right) v_i^{i^s}.$$

If the basis $\{v_i\}$ is holonomic $Q_{,i} = \partial Q / \partial x^i$.

We use a semicolon to denote absolute differentiation

$$T^a_{b';i} = T^a_{b',i} + L^a_{bi} T^b_{b'} - T^a_{a'} L^{a'}_{b'i}.$$

L is the linear connection of the principal space V; its components transform in the first two indices by the non-tensor rule

$$L^{a'}_{b'i} = v^{a'}_a v^a_{b',i} + v^{a'}_a L^a_{bi} v^b_{b'}$$

and in the third index by the tensor rule

$$L^a_{bi'} = L^a_{bi} v^i_{i'}.$$

The non-tensor rule is equivalent to the condition

$$v^a_{b';i} = v^a_{b',i} + L^a_{bi} v^b_{b'} - v^a_{a'} L^{a'}_{b'i} = 0.$$

It may be verified readily that

$$T^a_{b';i} = T^a_{b;i} v^b_{b'} = T^a_{b';i'} v^{i'}_i, \text{ etc.},$$

i.e. that $T_;$ is a tensor. This conservation of tensor character is a justification of the term "absolute differentiation."

---

[5] For a thoroughgoing abstract treatment of tangent spaces see Vanderslice, Am. Journal of Math., 56 (1934) 153–193, in particular §3 and §9.

Absolute differentiation extends at once to subspaces; for example,

$$T^a_{b_0;i} = T^a_{b_0,i} + L^a_{bi}T^b_{b_0} - T^a_{a_0}L^{a_0}_{b_0i}.$$

The connection L^0_0 of the subspace V_0 has components which transform in accordance with the rules given above for L.

3. **Osculating subspace.** The tensor $v_{0;}$ obtained from v_0 by absolute differentiation determines a subspace V_{0*}. This V_{0*} depends on the choice of the linear connection L^0_0 for V_0 but the sum $V_0 + V_{0*}$ does not. We call this sum the osculating subspace of V_0.

The subspace V_{0*} determined by the tensor $v_{0;}$ is the space of vectors which are linearly dependent on the columns of the matrix

$$\begin{Vmatrix} v^1_{1;1} & v^1_{1;2} & \cdots & v^1_{2;1} & \cdots & v^1_{m_0;n} \\ v^2_{1;1} & v^2_{1;2} & \cdots & v^2_{2;1} & \cdots & v^2_{m_0;n} \\ \vdots & \vdots & & \vdots & & \vdots \\ v^m_{1;1} & v^m_{1;2} & \cdots & v^m_{2;1} & \cdots & v^m_{m_0;n} \end{Vmatrix},$$

where of course

$$v^a_{b_0;i} = v^a_{b_0,i} + L^a_{bi}v^b_{b_0} - v^a_{a_0}L^{a_0}_{b_0i}.$$

Due to the tensor nature of $v_{0;}$ it does not matter with respect to what bases the components in the above matrix are calculated; the subspace V_{0*} is the same. We call

$$\text{osc } V_0 = V_0 + V_{0*}$$

the *osculating subspace* of V_0. V_{0*} is dependent on the choice of the connection L^0_0 for V_0 but osc V_0 is independent of this choice, as the above formula for $v^a_{b_0;i}$ shows. If osc V_0 coincides with V_0 we say that V_0 is self-parallel.

Let $V_0 = V_+ + V_-$. Then the tensor v_0 is linearly expressible in terms of the tensors v_+ and v_-, and $v_\pm$ in terms of v_0:

$$v^a_{a_0} = v^a_{a_+}t^{a_+}_{a_0} + v^a_{a_-}t^{a_-}_{a_0} \quad \text{and} \quad v^a_{a_\pm} = v^a_{a_0}t^{a_0}_{a_\pm}.$$

By absolute differentiation we get

$$v^a_{a_0;i} = v^a_{a_+;i}t^{a_+}_{a_0} + v^a_{a_+}t^{a_+}_{a_0;i} + v^a_{a_-;i}t^{a_-}_{a_0} + v^a_{a_-}t^{a_-}_{a_0;i} \quad \text{and} \quad v^a_{a_\pm;i} = v^a_{a_0;i}t^{a_0}_{a_\pm} + v^a_{a_0}t^{a_0}_{a_\pm;i}.$$

Therefore

$$\text{osc } V_0 \subset \text{osc } V_+ + \text{osc } V_- \quad \text{and} \quad \text{osc } V_\pm \subset \text{osc } V_0,$$

which shows that

$$\text{osc } (V_+ + V_-) = \text{osc } V_+ + \text{osc } V_-.$$

This addition theorem extends immediately to a sum of more than two subspaces.

The space osc V_0 is clearly left unchanged by an "affine" change of connection,

$$L^a_{bi} + 2v^a_b w_i \quad \text{in place of} \quad L^a_{bi}$$

(the general change preserving "parallelism"—see Eisenhart, loc. cit.,[2] p. 30). Hence our osculating subspace is an affine invariant.[6]

4. **Induced connection.** We say that L^0_0 is an *induced* connection if the subspace V_{0*} determined by $v_{0;}$ has no vectors in common with V_0. We find that any subspace complementary to V_0 within osc V_0 determines a unique induced connection L^0_0.

Let V_{0*} be an arbitrary subspace which has no vectors in common with V_0 but which is such that osc $V_0 = V_0 + V_{0*}$. Let $\{v_{a_{0*}}\}$ be a basis for V_{0*}. Then the equations

$$v^a_{b_0;i} = v^a_{b_0,i} + L^a_{bi} v^b_{b_0} - v^a_{a_0} L^{a_0}_{b_0 i} = v^a_{a_{0*}} L^{a_{0*}}_{b_0 i}$$

can be solved uniquely for $L^{a_0}_{b_0 i}$, $L^{a_{0*}}_{b_0 i}$. This means that V_{0*} is the subspace determined by $v_{0;}$ for a unique choice of L^0_0. Since by hypothesis V_{0*} is independent of V_0 this L^0_0 is an induced connection.

We notice that the affine change

$$L^a_{bi} + 2v^a_b w_i \quad \text{in place of} \quad L^a_{bi}$$

forces a corresponding change in an induced connection, viz.

$$L^{a_0}_{b_0 i} + 2v^{a_0}_{b_0} w_i \quad \text{in place of} \quad L^{a_0}_{b_0 i},$$

if V_{0*} is to remain the same.

In what follows we use induced connections exclusively.

---

[6] On the other hand the subspace $V_0 + V_{0*} + V_x$ (assuming the tangent space V_x to be a subspace of V) is a "projective" invariant of V_0, for it is left unchanged by a "projective" change of connection,

$$L^a_{bi} + v^a_b w_i + u_b v^a_i \qquad \text{in place of} \qquad L^a_{bi}.$$

As an illustration let our underlying space X be a curve in cartesian 4-space, let a local space of V be the 4-dimensional space of vectors issuing from a point on the curve, let a local space of V_0 be the line of vectors issuing from a point on the curve and tangent to a ruled surface passing through the curve, let the displacement of V be that determined by the 4-space in which everything lies, and let the displacement of V_0 be arbitrary. Then a local space of the osculating subspace $V_0 + V_{0*}$ is a plane which indicates how the generating line of the ruled surface is tending to turn about the curve; this plane is tangent to the ruled surface at infinity on the generating line. A local space of the projective osculating subspace $V_0 + V_{0*} + V_x$ is a 3-space which contains all the tangent planes to the ruled surface along a generating line. If the ruled surface is developable $V_0 + V_{0*}$ contains V_x and the 3-space becomes the plane of the affine osculant.

II. Decomposition

This part of the paper exploits the simple but fruitful notion of a decomposition of the principal space V into a set of mutually exclusive subspaces. Such a decomposition entails a corresponding decomposition of geometric objects in the principal space into geometric objects distributed among the subspaces.

5. **Decomposition of** L. We define a decomposition of V and examine the attendant decomposition of L.

Let our principal space V be decomposed into a set of independent subspaces $V_0, V_1, \cdots, V_w$, i.e.

$$V = V_0 + V_1 + \cdots + V_w \qquad \text{where } m = m_0 + m_1 + \cdots + m_w.$$

Associated with these subspaces we have two sets of tensors (cf. §1), $\{v^q_q\}$ and $\{v_q\}$, $0 \leqq q \leqq w$. From the equations

$$v^{a_q}_a v^a_{b_q} = v^{a_q}_{b_q} \, (= \delta^{a_q}_{b_q}) \quad \text{and} \quad v^{a_p}_a v^a_{b_q} = 0 \; (p \neq q)$$

we derive a third set of tensors, $\{v^q\}$.

We decompose L by the rule

$$L^{a_p}_{b_q i} = v^{a_p}_a (L^a_{bi} v^b_{b_q} + v^a_{b_q, i}) .$$

For $p = q$ this yields objects L^q_q which transform as linear connections. We accordingly adopt these L^q_q as the linear connections for the subspaces V_q of the decomposition. Then the above equation becomes

$$(\text{for } p = q) \quad 0 = v^{a_q}_a v^a_{b_q ; i} \quad \text{and} \quad (\text{for } p \neq q) \quad L^{a_p}_{b_q i} = v^{a_p}_a v^a_{b_q ; i} .$$

The latter stamps the $L^p_q (p \neq q)$ as tensors. Reversing these equations we get

$$\text{(F1)} \qquad v^a_{b_q ; i} = \sum_{p \neq q} v^a_{a_p} L^{a_p}_{b_q i} .$$

This shows that the L^q_q are induced connections.

Let $\{v_{a'}\}$ be a special basis for V formed from the vectors of the bases $\{v_{a_q}\}$ of the subspaces V_q, i.e. $\{v_{a'}\} = \sum \{v_{a_q}\}$. Then

$$\| v^a_{a'} \| = \| v^a_{a_0} v^a_{a_1} \cdots v^a_{a_w} \| \quad \text{and} \quad \| v^{a'}_a \| = \begin{Vmatrix} v^{a_0}_a \\ v^{a_1}_a \\ \cdot \\ \cdot \\ \cdot \\ v^{a_w}_a \end{Vmatrix} .$$

Comparing

$$L^{a'}_{b' i} = v^{a'}_a (L^a_{bi} v^b_{b'} + v^a_{b', i}) \quad \text{with} \quad L^{a_p}_{b_q i} = v^{a_p}_a (L^a_{bi} v^b_{b_q} + v^a_{b_q, i})$$

we see they are the same term for term; i.e.

$$\| L^{a'}_{b'i} \| = \left\| \begin{matrix} L^{a_0}_{b_0 i} & L^{a_0}_{b_1 i} & \cdots & L^{a_0}_{b_w i} \\ L^{a_1}_{b_0 i} & L^{a_1}_{b_1 i} & \cdots & L^{a_1}_{a_w i} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ L^{a_w}_{b_0 i} & L^{a_w}_{b_1 i} & \cdots & L^{a_w}_{b_w i} \end{matrix} \right\| .$$

The main diagonal contains the components of the induced connections L^q_q; elsewhere are the components of the tensors L^p_q. In like fashion

$$v^a_{b',i} + L^a_{bi} v^b_{b'} - v^a_{a'} L^{a'}_{b'i} = 0 \quad (\text{i.e. } v^a_{b';i} = 0)$$

and

$$v^a_{b_q,i} + L^a_{bi} v^b_{b_q} - v^a_{a_q} L^{a_q}_{b_q i} - \sum_{p \neq q} v^a_{a_p} L^{a_p}_{b_q i} = 0 \quad \left(\text{i.e. } v^a_{b_q;i} - \sum_{p \neq q} v^a_{a_p} L^{a_p}_{b_q i} = 0\right)$$

are the same term for term. We may therefore describe formula (F1) as a decomposition of $v_; = 0$. This important formula is a basis for formulas of the Frenet type.

Let $V_{0r} = V_0 + V_1 + \cdots + V_r$. Then $V = V_{0r} + V_{r+1} + \cdots + V_w$ is a decomposition of V into a set of independent subspaces which gives rise to the formula (cf. (F1))

$$v^a_{b_{0r};i} = \sum_{p > r} v^a_{a_p} L^{a_p}_{b_{0r} i} .$$

If $\{v_{a'_{0r}}\} = \sum_{q=0}^{r} \{v_{a_q}\}$ it is readily seen that

$$v^a_{b'_{0r},i} + L^a_{bi} v^b_{b'_{0r}} - v^a_{a'_{0r}} L^{a'_{0r}}_{b'_{0r} i} - \sum_{p > r} v^a_{a_p} L^{a_p}_{b'_{0r} i} = 0 \qquad \left(\text{i.e. } v^a_{b'_{0r};i} - \sum_{p > r} v^a_{a_p} L^{a_p}_{b'_{0r} i} = 0\right)$$

and

$$v^a_{b_q,i} + L^a_{bi} v^b_{b_q} - v^a_{a_q} L^{a_q}_{b_q i} - \sum_{p \neq q} v^a_{a_p} L^{a_p}_{b_q i} = 0 \qquad \left(\text{i.e. } v^a_{b_q;i} - \sum_{p \neq q} v^a_{a_p} L^{a_p}_{b_q i} = 0\right),$$

where $0 \leqq q \leqq r$, are the same term for term.

6. **Tensor decomposition.** We next examine the tensor decomposition which accompanies the decomposition of V. The considerations are mainly algebraic.

Let T be a mixed tensor of order two in V, and let

$$T^{a_p}_{b} = v^{a_p}_{a} T^a_b , \quad T^a_{b_q} = T^a_b v^b_{b_q} , \quad \text{and} \quad T^{a_p}_{b_q} = v^{a_p}_{a} T^a_b v^b_{b_q} .$$

These equations clearly define a decomposition of T into three sets of tensors: $\{T^p\}$, $\{T_q\}$, $\{T^p_q\}$. In particular, if $T = v$ the three sets are $\{v^p\}$, $\{v_q\}$, $\{v^p_q\}$, where $v^p_q = 0$ if $p \neq q$. Using the special basis $\{v_{a'}\} = \sum \{v_{a_q}\}$ we get

$$\| T^{a'}_{b'} \| = \left\| \begin{matrix} T^{a_0}_{b'} \\ T^{a_1}_{b'} \\ \cdot \\ \cdot \\ \cdot \\ T^{a_w}_{b'} \end{matrix} \right\| = \| T^{a'}_{b_0} T^{a'}_{b_1} \cdots T^{a'}_{b_w} \| = \left\| \begin{matrix} T^{a_0}_{b_0} & T^{a_0}_{b_1} & \cdots & T^{a_0}_{b_w} \\ T^{a_1}_{b_0} & T^{a_1}_{b_1} & \cdots & T^{a}_{b_w} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ T^{a_w}_{b_0} & T^{a_w}_{b_1} & \cdots & T^{a_w}_{b_w} \end{matrix} \right\| .$$

One proves the equality of these matrices by comparing

$$T^{a'}_{b'} = v^{a'}_{a} T^{a}_{b'} = T^{a'}_{b} v^{b}_{b'} = v^{a'}_{a} T^{a}_{b} v^{b}_{b'}$$

with

$$T^{a_p}_{b'} = v^{a_p}_{a} T^{a}_{b'}, \qquad T^{a'}_{b_q} = T^{a'}_{b} v^{b}_{b_q}, \qquad \text{and} \qquad T^{a_p}_{b_q} = v^{a_p}_{a} T^{a}_{b} v^{b}_{b_q}$$

and taking account of the special nature of $\| v^{a}_{a'} \|$ and $\| v^{a'}_{a} \|$ exhibited in §5.

In contrast to the above we point out that any part of a tensor which belongs to a subspace may also be regarded as belonging to the principal space directly. For example, the "upper part" of T^p belongs to a subspace; if we regard this as belonging to V directly we write $T^p = T^{(p)}$ where

$$T^{a(p)}_{b} = v^{a}_{a_p} T^{a_p}_{b} .$$

The subindex (p) in this equation modifies the T but not the a; i.e. the superscript of $T^{a(p)}_{b}$ refers to the basis $\{v_a\}$. Of course $T \not\approx T^{(p)}$ in general, but $T = \sum_p T^{(p)}$ as may readily be verified. Similarly $T = \sum_q T_{(q)} = \sum_p \sum_q T^{(p)}_{(q)}$.

Differentiating the last equation displayed above we get

$$T^{a(p)}_{b;i} = v^{a}_{a_p} T^{a_p}_{b;i} + v^{a}_{a_p;i} T^{a_p}_{b} .$$

This shows that in general $T^{(p)}_{;} \not\approx T^{p}_{;}$. Indeed the upper part of $T^{(p)}_{;}$ belongs to V essentially as well as nominally. However, decomposing it back into the subspace we get $T^{p}_{;}$, for

$$v^{a_p}_{a} T^{a(p)}_{b;i} = T^{a_p}_{b;i} \qquad \qquad (\text{since } v^{a_p}_{a} v^{a}_{b_p;i} = 0) .$$

7. **Decomposition of** R. We apply the tensor decomposition of the last section to the Riemann curvature tensor R of the principal space V.

By definition

$$R^{a}_{b\,i\,j} = (L^{a}_{b\,i,j} - L^{a}_{b\,j,i}) - (L^{a}_{ci} L^{c}_{bj} - L^{a}_{cj} L^{c}_{bi}) .$$

It is not difficult to verify that R is a tensor. R decomposes into the sets of tensors $\{R^p\}$, $\{R_q\}$, $\{R^p_q\}$. We are interested in the tensors R^p_q where

$$R^{a_p}_{b_q\,i\,j} = v^{a_p}_{a} R^{a}_{b\,i\,j} v^{b}_{b_q} .$$

Using the special basis $\{v_{a'}\} = \sum \{v_{a_q}\}$ we have (as with T in §6)

$$\| R^{a'}_{b'ij} \| = \left\| \begin{matrix} R^{a_0}_{b_0ij} & R^{a_0}_{b_1ij} & \cdots & R^{a_0}_{b_wij} \\ R^{a_1}_{b_0ij} & R^{a_1}_{b_1ij} & \cdots & R^{a_1}_{b_wij} \\ \vdots & \vdots & & \vdots \\ R^{a_w}_{b_0ij} & R^{a_w}_{b_1ij} & \cdots & R^{a_w}_{b_wij} \end{matrix} \right\| .$$

Hence

$$\text{(GC1)} \qquad R^{a_p}_{b_q ij} = (L^{a_p}_{b_q i,j} - L^{a_p}_{b_q j,i}) - \sum_r (L^{a_p}_{c_r i} L^{c_r}_{b_q j} - L^{a_p}_{c_r j} L^{c_r}_{b_q i}),$$

for the right side of this is term-for-term the same as the right side of (cf. §5)

$$R^{a'}_{b'ij} = (L^{a'}_{b'i,j} - L^{a'}_{b'j,i}) - (L^{a'}_{c'i} L^{c'}_{b'j} - L^{a'}_{b'j} L^{c'}_{b'i}) .$$

The formula (GC1) may accordingly be described as a decomposition of the formula expressing R in terms of L. It is a basis for formulas of the Gauss-Codazzi type.

A particular case of (GC1) is

$$R^{a_q}_{b_q ij} = \bar{R}^{a_q}_{b_q ij} - \sum_{r \neq q} (L^{a_q}_{c_r i} L^{c_r}_{b_q j} - L^{a_q}_{c_r j} L^{c_r}_{b_q i})$$

where $\bar{R}^q_q$ is the Riemann curvature tensor of the subspace V_q; i.e.

$$\bar{R}^{a_q}_{b_q ij} = (L^{a_q}_{b_q i,j} - L^{a_q}_{b_q j,i}) - (L^{a_q}_{c_q i} L^{c_q}_{b_q j} - L^{a_q}_{c_q j} L^{c_q}_{b_q i}) .$$

Another method of proving (GC1) is to differentiate (F1) by $(,j)$, take the skew-symmetric part, multiply by $v^{a_p}_a$ and sum on a. Operating with $(;j)$ one is led to the same result via the generalized Ricci identities

$$v^a_{b_q;ij} - v^a_{b_q;ji} + v^a_{b_q;k}(\Lambda^k_{ij} - \Lambda^k_{ji}) = R^a_{bij} v^b_{b_q} - v^a_{a_q} \bar{R}^{a_q}_{b_q ij} ,$$

where Λ denotes the linear connection of the tangent space V_x.

8. **Ordered decomposition.** By ordering the decomposition of our principal space V in terms of osculating subspaces we obtain a decomposition such that the tensors $L^p_q = 0$ for $p - q > 1$.

We choose the decomposition of V so that

$$V_0 + V_1 + \cdots + V_{q+1} = V_{0q+1} \supset \operatorname{osc} V_q$$

for all q. By the addition theorem of §3 this condition is equivalent to the condition that $V_{0q+1} \supset \operatorname{osc} V_{0q}$ for all q. Under this ordered decomposition (F1) takes the form

$$\text{(F2)} \qquad v^a_{b_q;i} = \sum_{p>q} v^a_{a_p} L^{a_p}_{b_q i} + v^a_{a_{q+1}} L^{a_{q+1}}_{b_q i} ,$$

since osc V_q is independent of $V_{q+2}, V_{q+3}, \cdots, V_w$. Hence

$$L^{a\,p}_{b\,q\,i} = v^{a\,p}_{a} v^{a}_{b\,q;i} = 0 \qquad \text{for} \qquad p - q > 1 .$$

Conversely we can show by retracing our steps that $L^p_q = 0$ for $p - q > 1$ and all q implies that $V_{0q+1} \supset \text{osc}\, V_q$ for all q. In (F2) we have a close approach to formulas of the Frenet type.

Under the ordered decomposition (GC1) becomes

$$
\text{(GC2)}\begin{cases}
R^{a\,p}_{b\,q\,ij} = (L^{a\,p}_{b\,q\,i,j} - L^{a\,p}_{b\,q\,j,i}) - \displaystyle\sum_{r=p-1}^{r=q+1} (L^{a\,p}_{c\,r\,i} L^{c\,r}_{b\,q\,j} - L^{a\,p}_{c\,r\,j} L^{c\,r}_{b\,q\,i}) & p < q \\
R^{a\,q}_{b\,q\,ij} = \bar{R}^{a\,q}_{b\,q\,ij} & \\
\qquad - (L^{a\,q}_{c\,q-1\,i} L^{c\,q-1}_{b\,q\,j} + L^{a\,q}_{c\,q+1\,i} L^{c\,q+1}_{b\,q\,j} - L^{a\,q}_{c\,q-1\,j} L^{c\,q-1}_{b\,q\,i} - L^{a\,q}_{c\,q+1\,j} L^{c\,q+1}_{b\,q\,i}) & \\
R^{a\,q+1}_{b\,q\,ij} = L^{a\,q+1}_{b\,q\,i;j} - L^{a\,q+1}_{b\,q\,j;i} & \\
R^{a\,q+2}_{b\,q\,ij} = L^{a\,q+2}_{c\,q+1\,i} L^{c\,q+1}_{b\,q\,j} - L^{a\,q+2}_{c\,q+1\,j} L^{c\,q+1}_{b\,q\,i} & \\
R^{a\,p}_{b\,q\,ij} = 0 \qquad p - q > 2 . &
\end{cases}
$$

In (GC2) we have a close approach to formulas of the Gauss-Codazzi type.

By recurrence we define the q^{th} *osculating subspace* of an arbitrary subspace V_0 as

$$\text{osc}_q\, V_0 = \text{osc}\, (\text{osc}_{q-1}\, V_0) \qquad \text{where} \qquad \text{osc}_0\, V_0 = V_0 .$$

If $\text{osc}_q\, V_0 = V$ then of course $\text{osc}_r\, V_0 = V$ for $r > q$; if $\text{osc}_q\, V_0$ is self-parallel (cf. §3) then $\text{osc}_r\, V_0 = \text{osc}_q\, V_0$ for $r > q$. We may assume therefore that the successive spaces $\text{osc}_q\, V_0$ are distinct for $q < w$ and that $\text{osc}_w\, V_0$ coincides with either V or $\text{osc}_{w-1}\, V_0$. We now choose $V_1, V_2, \cdots, V_w$ so that each V_q is complementary to $\text{osc}_{w-1}\, V_0$ within $\text{osc}_q\, V_0$, i.e. $V_q = (\text{osc}_{q-1}\, V_0)_*$ in the notation of §3; in particular, V_w is complementary to $\text{osc}_{w-1}\, V_0$ within V. These subspaces $V_0, V_1, \cdots, V_w$ form a decomposition of V of the ordered type described above.

III. Dual Considerations

Let u be a homogeneous linear function defined over the vectors of the space V, and let $u_a, u_{a'}$ be the values of u at the vectors $v_a, v_{a'}$ of the bases $\{v_a\}, \{v_{a'}\}$. Then

$$u_{a'} = u_a v^a_{a'} .$$

We recognize u as a tensor of order one with components $u_a, u_{a'}$ with respect to the bases $\{v_a\}, \{v_{a'}\}$. The aggregate of all such functions u is a vector space of m dimensions which we call the *dual* of V. It is customary to distinguish V from its dual by designating the elements of V as *contravariant vectors* and those of the dual as *covariant vectors*. In the following sections we consider both covariant and contravariant subspaces; the joint theory leads to new relationships.

9. **Covariant subspaces.** We first dualize the previous work to covariant subspaces. Once the necessary bases are established, this proceeds rapidly; omitted details can be supplied by analogy.

In §1 the components $v_a^{a'}$ had a vector as well as a tensor significance. Keeping a fixed and leaving a' free we had the components of a member v_a of a (contravariant) vector basis $\{v_a\}$ with respect to a (contravariant) basis $\{v_{a'}\}$. A vector $v_{a'}$ of the basis $\{v_{a'}\}$ has the components $v_{a'}^{a}$ with respect to the (contravariant) basis $\{v_a\}$. Here we follow a dual procedure. Keeping a' fixed and leaving a free in $v_a^{a'}$ we get the components of a member $v^{a'}$ of a covariant basis $\{v^{a'}\}$ with respect to a covariant basis $\{v^a\}$. A vector v^a of the basis $\{v^a\}$ has the components $v_{a'}^{a}$ with respect to the covariant basis $\{v^{a'}\}$. The transformation formulas are

$$v^{a'} = v_a^{a'} v^a \qquad \text{and} \qquad v^a = v_{a'}^{a} v^{a'} .$$

A covariant vector subspace V^0 is a linear subspace of m_0 dimensions of the dual of V. The notation for V^0 is obtained from that of the dual of V by the addition of a subzero. Let $\{v^{a_0}\}$ be a basis for V^0; then

$$v^{a_0} = v_a^{a_0} v^a .$$

$v_a^{a_0}$ are the components of the covariant basis vector v^{a_0} with respect to $\{v^\bullet\}$; also they are the components of a mixed tensor v^0.

Let L be the linear connection of the dual of V and let L_0^0 be the linear connection of V^0. Then

$$v_{b;i}^{a_0} = v_{b,i}^{a_0} + L_{b_0 i}^{a_0} v_b^{b_0} - v_a^{a_0} L_{b\,i}^{a} = - L_{b_{0*} i}^{a_0} v_b^{b_{0*}} ,$$

where v^{0*} is the fundamental tensor of the covariant subspace V^{0*} determined by $v_;^0$. Of course we define

$$\operatorname{osc} V^0 = V^0 + V^{0*}.$$

Let the dual of V be decomposed into a set of independent covariant subspaces:

$$\text{dual of } V = V^0 + V^1 + \cdots + V^w \qquad (m = m_0 + m_1 + \cdots + m_w) .$$

Associated with this decomposition there are two sets of tensors $\{v_p^p\}$, $\{v^p\}$. The equations

$$v_b^{a\,p} v_{b\;p}^{\,b} = v_{b\;p}^{a\,p} \,(= \delta_{b\;p}^{a\,p}) \qquad \text{and} \qquad v_b^{a\,p} v_{b\;q}^{\,b} = 0 \qquad (p \neq q)$$

define a third set $\{v_p\}$. We decompose L by the rule

$$L_{b\;q\,i}^{a\,p} = (v_a^{a\,p} L_{b\,i}^{a} - v_{b,i}^{a\,p}) v_{b\;q}^{\,b} .$$

Taking the L_p^p from these L_q^p as linear connections for the subspaces V^p we get

$$(\text{for } p = q) \qquad 0 = v_{b;i}^{a\,p} v_{b\;p}^{\,b} \qquad \text{and} \qquad (\text{for } p \neq q) \qquad L_{b\;q\,i}^{a\,p} = - v_{b;i}^{a\,p} v_{b\;q}^{\,b} .$$

Then, reversing these, we have

(F1′)
$$v^{a\,p}_{b;i} = -\sum_{q\neq p} L^{a\,p}_{b\,q\,i}\, v^{b\,q}_{b}.$$

The tensor decomposition which accompanies the decomposition of the dual of V is completely analogous to that introduced in §6. In particular, the decomposition of R leads to the formulas of §7.

If the decomposition of the dual of V is ordered so that

$$V^0 + V^1 + \cdots + V^{p+1} = V^{0p+1} \supset \text{osc } V^p$$

for all p, we find that

(F2′)
$$v^{a\,p}_{b;i} = -\sum_{q<p} L^{a\,p}_{b\,q\,i}\, v^{b\,q}_{b} - L^{a\,p}_{b\,p+1\,i}\, v^{b\,p+1}_{b}$$

and so, that

$$L^{a\,p}_{b\,q\,i} = -v^{a\,p}_{b;i}\, v^{b}_{b\,q} = 0 \quad \text{for } q - p > 1.$$

As a result of the latter the components of R^p_q $(q < p)$, R^p_p, R^p_{p+1}, R^p_{p+2}, and R^p_q $(q - p > 2)$ are expressible in forms similar to those displayed in (GC2).

10. **Dual subspaces.** In this section we study relations between covariant and contravariant subspaces.

By definition a covariant subspace V^0 and a contravariant subspace V_1 are *in involution* if

$$v^{a_0}_{a} v^{a}_{a_1} = 0.$$

This necessitates that $m_0 + m_1 \leqq m$. If $m_0 + m_1 = m$ the relationship is unique, i.e. given V^0 or V_1 a unique V_1 or V^0 is determined; if $m_0 + m_1 < m$ the relationship is not unique. Clearly the sum of two subspaces is in involution with a third if, and only if, each of the two subspaces is in involution with the third. Differentiating the above equation we get

$$v^{a_0}_{a} v^{a}_{a_1;i} + v^{a_0}_{a;i} v^{a}_{a_1} = 0.$$

Hence V^0 and V_{1*} (cf. §3) are in involution if, and only if, V^{0*} and V_1 are. Moreover, still assuming V^0 and V_1 in involution, we see that V^0 and osc V_1 are in involution if, and only if, V_1 and osc V^0 are in involution.

By definition a covariant subspace V^0 and a contravariant subspace V_0 are *dual* if no part of one is in involution with the other. This requires that the two subspaces have the same dimension and that $|v^{a_0}_{a} v^{a}_{b_0}| \neq 0$; when such is the case we may assume the bases $\{v^a\}$ $\{v_a\}$ so chosen that

$$v^{a_0}_{a} v^{a}_{b_0} = \delta^{a_0}_{b_0} (= v^{a_0}_{b_0}).$$

Duality between subspaces is not unique, i.e. given V^0 or V_0 a unique dual subspace V_0 or V^0 is not intrinsically determined; the equation just displayed shows the degree of arbitrariness.

A pair of dual subspaces V^0, V_0 have a unique connection determined by

$$L^{a_0}_{b_0 i} = v^{a_0}_a (L^a_{bi} v^b_{b_0} + v^a_{b_0, i}) = (v^{a_0}_a L^a_{bi} - v^{a_0}_{b, i}) v^b_{b_0}.$$

Adopting this connection these equations become

$$0 = v^{a_0}_a v^a_{b_0 ; i} = -v^{a_0}_{b ; i} v^b_{b_0}.$$

Hence V^0 and V_{0*} are in involution, as are V^{0*} and V_0. This means that V_{0*} is independent of V_0 and that V^{0*} is independent of V^0. In other words our L^0_0 is an induced connection for both V^0 and V_0. Of course V^{0*} and V_{0*} are not in general dual; they may even differ in dimension. The same is true of osc V^0 and osc V_0.

A pair of dual subspaces V^0, V_0 jointly determine a convenient unit for tensor reference; thus

$$T^{a_0}_b = v^{a_0}_a T^a_b, \qquad T^a_{b_0} = T^a_b v^b_{b_0}, \qquad T^{a_0}_{b_0} = v^{a_0}_a T^a_b v^b_{b_0}, \qquad T^{c(0)}_b = v^a_{a_0} T^{a_0}_b$$

$$T^{c(0)}_{b ; i} = v^a_{a_0} T^{c_0}_{b ; i} + v^a_{a_0 ; i} T^{a_0}_b, \qquad v^{a_0}_a T^{a(0)}_{b ; i} = T^{a_0}_{b ; i}, \text{ etc.}$$

11. **Dual decomposition.** We decompose V and the dual of V into dual sets of independent subspaces. By ordering this dual decomposition in terms of osculating subspaces we get a decomposition of especial interest.

Consider a dual decomposition into independent subspaces

$$\begin{aligned} \text{dual of } V &= V^0 + V^1 + \cdots + V^w \\ V &= V_0 + V_1 + \cdots + V_w \end{aligned} \qquad (m = m_0 + m_1 + \cdots + m_w)$$

such that V^p and V_q are dual if $p = q$ and in involution if $p \neq q$. Then

$$v^{a_q}_a v^a_{b_q} = v^{a_q}_{b_q} (= \delta^{a_q}_{b_q}) \quad \text{and} \quad v^{a_p}_a v^a_{b_q} = 0 \quad p \neq q.$$

From these equations one sees that a knowledge of one part of the decomposition, either covariant or contravariant, determines the other part. It is to be noticed that $V^{0q} = V^0 + V^1 + \cdots + V^q$ and $V_{0q} = V_0 + V_1 + \cdots + V_q$ are dual subspaces.

Under this dual decomposition L decomposes by the concordant rules

$$L^{a_p}_{b_q i} = v^{a_p}_a (L^a_{bi} v^b_{b_q} + v^a_{b_q, i}) = (v^{a_p}_a L^a_{bi} - v^{a_p}_{b, i}) v^b_{b_q}.$$

The L^p_p are induced connections for the pairs V^p, V_p. Using these we have

$$v^{a_q}_a v^a_{b_q ; i} = 0 = v^{a_p}_{b ; i} v^b_{b_p} \quad \text{and} \quad L^{a_p}_{b_q i} = v^{a_p}_a v^a_{b_q ; i} = -v^{a_p}_{b ; i} v^b_{b_q} \quad \text{if } p \neq q,$$

from which follow

$$v^a_{b_q ; i} = \sum_{p \neq q} v^a_{a_p} L^{a_p}_{b_q i} \quad \text{and} \quad v^{a_p}_{b ; i} = -\sum_{q \neq p} L^{a_p}_{b_q i} v^{b_q}_b.$$

Tensor decomposition is as in §6, and so R decomposes as in §7.

Let the decomposition of V be such that

$$\text{a) } \operatorname{osc} V_q \subset V_{0q+1} \quad (\text{or } \operatorname{osc} V_{0q} \subset V_{0q+1}) \quad \text{for all } q.$$

Then for $p - q > 1$ the subspaces V^p are in involution with osc V_q and so with V_{q*}. Therefore

$$L^{a\,p}_{b\,q\,i} = v^{a\,p}_{a} v^{a}_{b\,q;i} = 0 \quad \text{for } p - q > 1.$$

Let the decomposition of the dual of V be such that

$$\text{b) } \operatorname{osc} V^p \subset V^{0p+1} \quad (\text{or } \operatorname{osc} V^{0p} \subset V^{0p+1}) \quad \text{for all } p.$$

Then for $q - p > 1$ the subspaces V_q are in involution with osc V^p and so with V^{p*}. Therefore

$$L^{a\,p}_{b\,q\,i} = -v^{a\,p}_{b;i} v^{b}_{b\,q} = 0 \quad \text{for } q - p > 1.$$

Taken together a) and b) necessitate that

$$L^{a\,p}_{b\,q\,i} = 0 \quad \text{for } |p - q| > 1.$$

Hence

$$\text{(F3)} \quad v^{a}_{b\,q;i} = v^{a}_{a_{q-1}} L^{a\,q-1}_{b\,q\,i} + v^{a}_{a_{q+1}} L^{a\,q+1}_{b\,q\,i} \quad \text{and} \quad v^{a\,p}_{b;i} = -L^{a\,p}_{b\,p-1\,i} v^{b\,p-1}_{b} - L^{a\,p}_{b\,p+1\,i} v^{b\,p+1}_{b}.$$

Also

$$\text{(GC3)} \begin{cases} R^{a\,q}_{b\,q\,ij} = \bar{R}^{a\,q}_{b\,q\,ij} - (L^{a\,q}_{c\,q-1\,i} L^{c\,q-1}_{b\,q\,j} + L^{a\,q}_{b\,q+1\,i} L^{c\,q+1}_{b\,q\,j} - L^{a\,q}_{c\,q-1\,j} L^{c\,q-1}_{b\,q\,i} - L^{a\,q}_{c\,q+1\,j} L^{c\,q+1}_{b\,q\,i}) \\ R^{a\,q\pm1}_{b\,q\,i\,j} = L^{a\,q\pm1}_{b\,q\,i;j} - L^{a\,q\pm1}_{b\,q\,j;i} \\ R^{a\,q\pm2}_{b\,q\,i\,j} = L^{a\,q\pm2}_{c\,q\pm1\,i} L^{c\,q\pm1}_{b\,q\,j} - L^{a\,q\pm2}_{c\,q\pm1\,j} L^{c\,q\pm1}_{b\,q\,i} \\ R^{a\,p}_{b\,q\,ij} = 0 \qquad |p - q| > 2. \end{cases}$$

In (F3) we have formulas definitely of the Frenet type, and in (GC3) of the Gauss-Codazzi type.

Starting from an arbitrary pair of dual subspaces V^0, V_0 a dual decomposition satisfying a) and b) can be built up in the following recurrent fashion. We suppose that we have subspaces $V^1, V_1; V^2, V_2; \cdots; V^r, V_r$ such that V^p and V_q are dual if $p = q$ and in involution if $p \neq q$ and such that osc $V^{p-1} \subset V^{0p}$ and osc $V_{q-1} \subset$ osc V_{0q} (for $p, q \leqq r$); moreover we suppose that the dimensions $m_1, m_2, \cdots, m_r$ are the minimal ones for such a system. Let $V^\Gamma = V^{0r*}$ and $V_\Delta = V_{0r*}$ be the subspaces determined by the dual subspaces V^{0r}, V_{0r} and the unique induced connection L^{0r}_{0r} (cf. §9) and let $\rho = \operatorname{rank} \| v^{a\Gamma}_{a} v^{a}_{a_\Delta} \|$. Then $m_\Gamma - \rho$ is the dimension of the part V^γ of V^Γ which is in involution with V_Δ, and $m_\Delta - \rho$ is the dimension of the part V_δ of V_Δ with which V^Γ is in involution. Let V^δ be a subspace dual to V_δ and in involution with V_{0r}, and let V_γ be a subspace with which V^γ is dual and V^{0r} is in involution. Then $V^{r+1} = V^\Gamma + V^\delta$ and $V_{r+1} = V_\Delta + V_\gamma$ are dual with the minimal dimension $m_{r+1} = m_\Gamma + m_\Delta - \rho$

such that both V^{r+1} and V^{0r} are in involution with V_{0r} and V_{r+1}, respectively, and such that osc $V^{0r} \subset V^{0r+1}$ and osc $V_{0r} \subset V_{0r+1}$. We have thus enlarged the above system of subspaces by a new pair V^{r+1}, V_{r+1}. This process can be continued until we get $V_{0w} = V$ or V^{0w-1} and V_{0w-1} both self-parallel; in the latter case we complete the system by an arbitrary pair of dual subspaces V^w, V_w which are in involution with V_{0w-1} and V^{0w-1}. The dual decomposition satisfying a) and b), which is thus obtained, is the nearest non-Riemannian approach to the Riemannian notion of a subspace and its successive normal subspaces (cf. §12, 13). The arbitrariness in the decomposition, assuming the dual pair V^0, V_0 given, occurs in the choice of the subspaces V^δ, V_γ at each step; however either or both of these may be vacuous.

IV. Special Cases

The final part of this paper deals with spaces which possess more definite structure than we have hitherto considered. In particular, we show the relation of the previous work to the more familiar theory of Riemannian subspaces.

12. Orthogonality. Let us suppose that in some way we have a one-to-one correspondence between the contravariant subspaces of V and the covariant subspaces of the dual of V, and that this correspondence is such that

1) corresponding subspaces V^0, V_0 are dual,
2) if V^0 and V_1 are in involution the corresponding subspaces V_0 and V^1 are in involution, and conversely,
3) V^{0*}, V_{0*} correspond if V^0, V_0 do.

V^{0*}, V_{0*} are determined by using the unique induced connection L_0^0 associated with the dual pair V^0, V_0 (cf. §10).

We say that one subspace (V_0 or V^0) is *orthogonal* to another (V_1 or V^1) if the first is in involution with the subspace (V^1 or V_1) corresponding to the second. Due to 2) this relationship is symmetric. We exhibit the situation by a table

V^0	orthogonal to	V^1
dual to	in involution with	dual to
V_0	orthogonal to	V_1

which contains six statements: two horizontal, two diagonal, and two vertical. If V^0, V^1 correspond to V_0, V_1 and if one of the horizontal or diagonal statements is true then all six statements are true. When $m_0 + m_1 = m$ the involution is unique and so all four subspaces are determined if just one is given. In other words each subspace has a unique orthogonal complement.

The sum of two subspaces is orthogonal to a third subspace if, and only if, each of the two is orthogonal to the third, for the sum of the two is in involution with the subspace corresponding to the third if, and only if, each of the two is in involution with that subspace. Hence the orthogonal complement of the

sum of two subspaces is the common part of the orthogonal complements of the two. This enables us to conclude that the subspace corresponding to the sum of two subspaces is the sum of the subspaces corresponding to the two.

We say that a decomposition of V or of the dual of V is orthogonal if every two subspaces of the decomposition are orthogonal. The relations embodied in the above table show that the subspaces corresponding to those of an orthogonal decomposition of V form an orthogonal decomposition of the dual of V, and conversely; the two decompositions taken together form an orthogonal dual decomposition.

The subspaces V^{0*}, V_{0*} derived from a pair of corresponding subspaces V^0, V_0 are in involution with V_0, V^0, and due to 3) they correspond. Hence V^0, V_0 and $V^1 = V^{0*}$, $V_1 = V_{0*}$ fit the above table. $V^{01} = V^0 + V^1$ and $V_{01} = V_0 + V_1$ correspond. Let $V^2 = V^{01*}$ and $V_2 = V_{01*}$. Continuing this process we get a unique orthogonal dual decomposition arising from V^0, V_0. The general terms in the decomposition are

$$V^{p+1} = V^{0p*}, \qquad\qquad V_{q+1} = V_{0q*}.$$

If we encounter $V^{0r} = 0 = V_{0r}$ before the decomposition is complete we write $r = w - 1$ and take the orthogonal complements of V^{0r}, V_{0r} as the final subspaces V^w, V_w. We call the subspaces V^q, V_q of this orthogonal dual decomposition the q^{th} *normal subspaces* of V^0, V_0. The subspaces V^{0q}, V_{0q} are the q^{th} osculating subspaces of V^0, V_0. Formulas (F3) and (GC3) apply to this decomposition.

13. **Riemannian subspaces.** We now assume that there is a Riemannian metric g associated with V and the dual of V. We show that g determines a correspondence of the type discussed in the preceding section. This correspondence is a part of a system of raising and lowering indices to which g gives rise.

The Riemannian metric g is a symmetric non-singular tensor, or pair of tensors, with components

$$g_{ab} = g_{ba}, \qquad g^{ab} = g^{ba}, \qquad \text{where} \qquad g^{ab}g_{bc} = \delta^a_c.$$

It combines with L so that

$$g_{ab;i} = 0, \qquad g^{ab}_{;i} = 0,$$

one of these being a consequence of the other.

The equations

$$v^{a_0}_b = g_{ab}v^a_{b_0}g^{a_0b_0}, \qquad v^a_{b_0} = g_{a_0b_0}v^{a_0}_b g^{ab},$$

where

$$g_{a_0b_0} = g_{ab}v^a_{a_0}v^b_{b_0}, \qquad g^{a_0b_0} = v^{a_0}_a v^{b_0}_b g^{ab},$$

$$g^{a_0b_0}g_{b_0c_0} = \delta^{a_0}_{c_0},$$

serve to determine both $v_b^{a_0}$ and $v_{b_0}^a$ provided either is given. This means that g determines a one-to-one correspondence between the contravariant subspaces of V and the covariant subspaces of the dual of V. This correspondence satisfies condition 1) of the preceding section since

$$v_a^{a_0} v_{b_0}^a = \delta_{b_0}^{a_0} \ (= v_{b_0}^{a_0})$$

is a consequence of the above equations. The correspondence also satisfies condition 2) for by using the equations at the beginning of this paragraph with subone as well as subzero we see that

$$v_a^{a_0} v_{a_1}^a = 0 \qquad \text{if, and only if,} \qquad v_a^{a_1} v_{a_0}^a = 0 .$$

At the same time we have that

$$g_{a_0 b_1} = g_{ab} v_{a_0}^a v_{b_1}^b = 0 \qquad \text{if, and only if,} \qquad g^{a_0 b_1} = v_a^{a_0} v_b^{b_1} g^{ab} = 0 .$$

The first of these is the condition that V_0 and V_1 are orthogonal, and the second that V^0 and V^1 are orthogonal.

We use g to raise and lower indices according to the following system:

$$T_{a_0 b} = g_{a_0 b_0} T_b^{b_0}, \qquad\qquad T^{a_0 b} = T_a^{a_0} g^{ab}$$

$$T_a^{a_0} = g_{ab} T^{a_0 b} = T_{b_0 a} g^{a_0 b_0}$$

$$T_{a_0}^{\cdot a} = g_{a_0 b_0} T^{b_0 a} = T_{a_0 b} g^{ab}, \text{ etc.}$$

In this notation

$$v_b^{\cdot a_0} = v_b^{a_0} \qquad \text{and} \qquad v_{b_0}^{\cdot a} = v_{b_0}^a$$

as the work of the last paragraph shows. If we are to have

$$T_{a_0; i}^{\cdot a} = g_{a_0 b_0} T_{b; i}^{b_0} g^{ab}, \text{ etc.,}$$

i.e. if the operations of raising and lowering indices by g are to commute with absolute differentiation, we must have

$$g_{ab;i} = 0, \qquad g_{;i}^{ab} = 0; \qquad g_{a_0 b_0; i} = 0, \qquad g_{;i}^{a_0 b_0} = 0; \qquad \text{etc.}$$

The first tvo of these are true by hypothesis; the others follow from the first two, for

$$g_{a_0 b_0; i} = g_{ab} v_{a_0}^a v_{b_0; i}^b + g_{ab} v_{a_0; i}^a v_{b_0}^b = 0$$

since V^0 is in involution with V_{0*}, and

$$g_{;i}^{a_0 b_0} = v_a^{a_0} v_{b; i}^{b_0} g^{ab} + v_{a; i}^{a_0} v_b^{b_0} g^{ab} = 0$$

since V_0 is in involution with V^{0*}. Of course the connection L_0^0 here used is the unique induced connection associated with the dual subspaces V^0, V_0.

If V^0, V_0 are orthogonal to V^1, V_1 we have

$$0 = (v_a^{a_0} v_{b_1}^a)_{;i} = v_a^{a_0} v_{b_1;i}^a + v_{a;i}^{a_0} v_{b_1}^a = L_{b_1 i}^{a_0} + L_{b_1 i}^{\cdot a_0}$$

$$0 = g_{a_0 b_1;i} = g_{ab} v_{a_0}^a v_{b_1;i}^b + g_{ab} v_{a_0;i}^a v_{b_1}^b = L_{a_0 b_1 i} + L_{b_1 a_0 i}\,.$$

Hence

$$L_{b_1 i}^{\cdot a_0} = - L_{b_1 i}^{a_0} \qquad \text{and} \qquad L_{b_1 a_0 i} = - L_{a_0 b_1 i}\,.$$

In particular, we see that the formulas

$$v_{b_0;i}^a = v_{a_{0*}}^a L_{b_0 i}^{a_{0*}} = - v_{a_{0*}}^a L_{b\,i}^{\cdot a_{0*}}$$

$$v_{b;i}^{a_0} = L_{b_{0*}}^{\cdot a_0} v_b^{b_{0*}} = - L_{b_{0*} i}^{a_0} v_b^{b_{0*}}$$

differ merely by shift of indices. Therefore condition 3) of the preceding section is satisfied by the one-tc-one correspondence determined by g.

For the Riemannian situation considered here formulas (F3) can be written in the following form[7] which definitely reveals their Frenet character:

$$\text{(F4)} \qquad \begin{cases} v_{b;i}^{a\,p} = g_{a_{p+1} b_{p+1}} L_i^{b_{p+1} a_p} v_b^{a_{p+1}} - g_{a_{p-1} b_{p-1}} L_i^{a_p b_{p-1}} v_b^{a_{p-1}} \\ v_{b_q;i}^{a} = v_{b_{q+1}}^{a} L_{a_{q+1} b_q i}\, g^{a_{q+1} b_{q+1}} - v_{b_{q-1}}^a L_{b_q a_{q-1} i}\, g^{a_{q-1} b_{q-1}}\,. \end{cases}$$

These two formulas differ merely by shift of indices. They apply of course to an orthogonal dual decomposition such that

$$\operatorname{osc} V^p \subset V^{0p+1}, \qquad \operatorname{osc} V_q \subset V_{0q+1} \qquad (0 \leqq p, q \leqq w).$$

In the present Riemannian situation one of these conditions implies the other. A familiar case of such a decomposition is that provided by V^0, V_0 and their successive normal subspaces (cf. end of §12).

14. **Tangent spaces.** So far we have not considered the familiar ("holonomic") case in which one or more of our spaces have local spaces which are tangent to underlying spaces. But such a particularization makes little difference in our work as the following considerations show.

Suppose the tangent space V_x of our underlying space X is a contravariant subspace of V, i.e. that the vectors of a basis $\{v_i\}$ for V_x are expressible in terms of a basis $\{v_a\}$,

$$v_i = v_a v_i^a\,.$$

Then the ideas we have developed for any contravariant subspace of V apply to V_x. We have only to set $V_x = V_0$ in the previous work to get automatically

[7] Cf. Duschek and Mayer, *Lehrbuch der Differentialgeometrie* II (1930); Schouten and van Kampen, Math. Ann. 105 (1931), 144–159; Cutler, Trans. Am. Math. Soc. 33 (1931), 839–850.

for V_x the theory of successive osculating subspaces, formulas of the Frenet and Gauss-Codazzi type, etc.

Suppose we have another underlying space Y (of points y) which contains the underlying space X as a subspace, and suppose that V, etc., are functions of y as well as of x. Let V_y be the tangent space of the underlying space Y, and let $\{v_\alpha\}$ be a reference frame for V_y. Then

$$v_i = v_\alpha v^\alpha_i,$$

where $v^\alpha_i = \partial y^\alpha/\partial x^i$ if $\{v_\alpha\}$ and $\{v_i\}$ are both holonomic bases. Of course

$$T^{a_1}_{b,i} = T^{a_1}_{b,\alpha} v^\alpha_i$$

and so

$$T^{a_1}_{b;i} = T^{a_1}_{b;\alpha} v^\alpha_i$$

if

$$L^a_{b\,i} = L^a_{b\,\alpha} v^\alpha_i \qquad \text{and} \qquad L^{a_1}_{b_1 i} = L^{a_1}_{b_1 \alpha} v^\alpha_i$$

as we naturally assume.

Finally, suppose $V = V_y$. Then V_x is automatically a contravariant subspace of V. This is the most familiar instance of a subspace in differential geometry.

PRINCETON UNIVERSITY,
PRINCETON, NEW JERSEY.

ANNALS OF MATHEMATICS
Vol. 36, No. 4, October, 1935

ON AUTOMORPHISMS OF CERTAIN RINGS

BY JAKOB LEVITZKI

(Received March 28, 1934)

Introduction. The purpose of the present paper is to derive some properties of a ring (in short: I-ring) in which the *chain conditions on the right ideals* (see §1) hold concerning its automorphisms. A special case of this problem arises by the study of a normal product of two algebras A and B over a field F.[1] If A is the normal and B the supplementary factor, then A possesses a basis $a_1, a_2, \cdots, a_n$ over F such that $a_iB = Ba_i, i = 1, \cdots, n$. These relations define automorphisms of the algebra B, and it is of importance to study the behaviour of B under these automorphisms in order to know the structure of the normal product.

First we consider in this note a finite or infinite set M of automorphisms of a I ring R. If K denotes the *kernel* of R (i.e. the set of all the elements which remain invariant under each automorphism which belongs to M), then we prove that the quotient-ring K/N, where N is the radical of K, is semi-simple—i.e. the chain condition holds. We then assume that M is a finite group and that $na \neq 0$ for $a \neq 0$, where $a \in R$ and n is the order of the group M. In this case we prove that the kernel of a I ring R is a potent ring if, and only if the ring R is potent. There exists a one to one correspondence between the *primitive* right ideals of K and the *normal-primitive* right ideals of R, i.e. the minimal potent right-ideals of R which remain invariant under each automorphism of R belonging to M; further, the radical of the kernel is a subset of the radical of R. We further prove that the kernel of a semi simple ring is also a semi simple ring. Finally, a new proof is derived for the theorem which states that the group algebra of a finite group over a field F is semi simple.

For a detailed study of the notions used in this paper, consult B. L. v. d. Waerden, *Moderne Algebra*, II, pp. 149–172.

I. PRELIMINARY REMARKS AND DEFINITIONS

1. A ring R in which the "chain conditions on right ideals" are fulfilled, or in short: a I-ring, is a ring with the following properties: For each sequence $A_1, A_2, \cdots$ of right ideals of R, where either $A_i \subseteq A_k$ for $i \leqq k$ or $A_i \supseteq A_k$ for $i \geqq k$ there exists an integer r such that $A_s = A_t$ if $s, t \geqq r$.

A ring R with a radical N (i.e. N is the maximal nilpotent ideal, which contains all the nilpotent right and left ideals; a subring or an ideal of a ring is called nilpotent if some power of it is zero) whose quotient ring R/N with respect to N is semi simple, will be called in the following a II-ring.

[1] For the definition of normal products see: J. Levitzki, *On normal products of algebras*, Annals of Mathematics, vol. 33, pp. 377–402.

2. We cite without proofs the following known facts:

Each right ideal $A \neq 0$ of a I ring R has a finite length, i.e. a finite set of right ideals $A_2, \cdots, A_\lambda$ can be found such that $A = A_1 \supset A_2 \supset \cdots \supset A_\lambda = 0$ and if $1 \leqq i < \lambda$ then the right ideal A_{i+1} is a maximal right ideal which is different from A_i and is a subset of A_i; the integer λ is uniquely determined and is called the length of the right ideal A.

Each potent right ideal of a II ring R contains a primitive, i.e. a minimal potent right ideal of R.

Each primitive right ideal A of a II ring possesses a left hand unit e, i.e. $eA = A, e^2 = e$.

Each potent right ideal A of a II ring contains a principal idempotent element e, i.e. there exists a representation of A as a direct sum: $A = eA + B$, where the right ideal B is contained in the radical of R.[2]

If A is a right ideal of a I ring R and $a \varepsilon R$ such that $aA = A$, then A does not contain zero divisors of a, i.e. from $ab = 0$, $b \varepsilon A$ follows $b = 0$.[3]

If in addition $a \varepsilon A$, then A contains an idempotent element e such that $a = ae$. From $aA = A$, $a \varepsilon A$ it follows namely that $ae = a$, where $e \varepsilon A$; hence $ae^2 = ae = a$ and $a(e^2 - e) = 0$, where $(e^2 - e) \varepsilon A$. From the theorem just cited follows $e^2 - e = 0$, or $e^2 = e$, q.e.d.

3. If d_1 and d_2 are principal idempotent elements of a I ring R, then the following relations hold: $d_2d_1 = d_1 + c_1$, $d_1d_2 = d_2 + c_2$, where c_1 and c_2 are elements of the radical of R. This fact follows easily from the definition of principal idempotent elements.

4. If $d_1, \cdots, d_n$ are principal idempotent elements of a I ring R and if the relation $na = 0$ where $a \varepsilon R$ always implies $a = 0$, then $\sum_{i=1}^{n} d_i$ is a potent element. We first prove that $c = \sum_{i=1}^{n} d_i$ is not an element of the radical N of R. From $\sum_{i=1}^{n-1} d_i - c = -d_n$ follows namely $(\sum_{i=1}^{n-1} d_i - c)^2 = d_n$. On the other hand $(\sum_{i=1}^{n-1} d_i - c)^2 = (n-1)\sum_{i=1}^{n-1} d_i + c^*$ where (according to 3) $d_i d_k = d_k + c_{ik}$, $c_{ik} \varepsilon N$ and $c^* = c^2 - \sum_{i=1}^{n-1} d_i c - c\sum_{i=1}^{n-1} d_i + \sum_{i,k=1}^{n-1} c_{ik}$, hence $c^* \varepsilon N$ if $c \epsilon N$. From $\sum_{i=1}^{n-1} d_i = -d_n + c$, or $(n-1)\sum_{i=1}^{n-1} d_i = -(n-1)d_n + (n-1)c$ in connection with $(n-1)\sum_{i=1}^{n-1} d_i + c^* = d_n$ follows $nd_n = \bar{c}$, where $\bar{c} = c^* + (n-1)c$, hence $\bar{c} \varepsilon N$. If now $\bar{c}^\lambda = 0$, then also $n^\lambda d_n = 0$, hence in virtue of the assumption made, $n^{\lambda-1} d_n = 0$ (if $\lambda > 1$); similarly we obtain the contradictory result $d_n = 0$. Hence c is not an element of N. From $d_i d_k = d_k + c_{ik}$ with $c_{ik} \varepsilon N$ follows $c^2 = nc + c_1$ where $c_1 \varepsilon N$ and in general: $c^\nu = n^\nu c + c_{\nu-1}$ where $c_{\nu-1} \varepsilon N$ for each integral ν. The theorem will be proved if we show that together with c also $n^{\nu-1} c$ does not lie in N. The potent right

[2] For the proofs of these theorems consult G. Koethe, *Die Struktur der Ringe deren Restklassenring nach dem Radikal vollständig reduzibel ist.* Math. Zeitschrift Bd. 32, S, 161–186.

[3] For the proof of this theorem see E. Artin, *Zur Theorie der hyperkomplexen Zahlen,* Abhandl. d. math. Sem. d. Universität Hamburg, 5 (1927) p. 251–260.

ideal cR contains namely an idempotent element e, hence the right ideal $n^{\nu-1}cR$ contains the element $n^{\nu-1}e$ which is evidently a potent element (since $(n^{\nu-1}e)^{\mu} = n^{(\nu-1)\mu}e$ for each intergral μ), hence $n^{\nu-1}c$ does not lie in the radical, which completes the proof of the theorem.

5. If n is the length of the I ring R, and if the product of $n+1$ elements $a_1, \cdots, a_n$, in the given order differs from zero, then there exists a potent element p in R which has the form $p = b_1 b_2 \cdots b_m$ where the b_i are elements of the system $a_1, \cdots, a_{n+1}$. Each nilring, i.e. a ring whose elements are nilpotent, which is a subset of a I ring, is a nilpotent ring.

Each subring of a I ring contains a radical.[4]

6. If R is a I ring and R' is a subring of R in which every potent right ideal contains an idempotent element, then the quotient ring of R' with respect to its radical (which exists according to 5) is a semi simple ring.

If, namely, A' is a potent right ideal in R', then we show that A' contains a primitive right ideal of R'. Let namely e_1 be an idempotent element in A', then $e_1R' \subseteq A'$. If e_1R' is primitive, then the statement is true. Otherwise let A_1' be a potent right ideal such that $A_1' \subset e_1R'$. Let e_2 be an idempotent element in A_1', then $e_2R' \subset e_1R'$; Similarly we prove either the existence of a primitive right ideal of R' which is contained in A', or we prove the existence of an infinite sequence of right ideals e_iR', $i = 1, 2, \cdots$ in R' such that $e_1R' \supset e_2R' \supset \cdots$ and $e_i^2 = e_i$, $i = 1, 2, \cdots$. From $e_iR' \supset e_{i+1}R'$ follows $(e_iR', e_iR'R) \supseteq (e_{i+1}R', e_{i+1}R'R)$; but since $e_\lambda R'R = e_\lambda R'$ (this is a consequence of $e_\lambda R = e_\lambda e_\lambda R \subseteq e_\lambda R'R$ and $e_\lambda R'R \subseteq e_\lambda R$) and $e_\lambda R' \subseteq e_\lambda R$ we have $(e_\lambda R', e_\lambda R'R) = e_\lambda R$: hence, from $e_iR' \supset e_{i+1}R'$ follows $e_iR \supseteq e_{i+1}R$. Since $e_iR = e_{i+1}R$ implies $e_{i+1}e_i = e_i$ and hence $e_{i+1}R' \supseteq e_{i+1}e_iR' = e_iR'$ and this in its turn contradicts $e_{i+1}R' \subset e_iR'$, we obtain $e_iR \supset e_{i+1}R$ for each integral i. But this contradicts the assumption that R is a I ring. Hence the right ideal A' of R' contains a primitive right ideal of R'. The usual methods now lead easily to the proof of the theorem.

7. Definitions. If R is a I ring and M a finite or infinite set of automorphisms of R, then each subset of R which is transformed into itself under each automorphism of R which lies in M, is called a *normal subset* of R (with respect to M). Normal subrings, ideals, left and right ideals are defined similarly. The set K of all the elements of R which are invariant under M, is called the *kernel* of R (with respect to M). The kernel is evidently a ring.

A right ideal A of R is called *normal primitive* (with respect to M) if A is potent, and a normal subset of R, and if in A no other right ideals with the same property are contained except A itself.

---

[4] For the theorems cited in 5 compare J. Levitzki, *Über nilpotente Unterringe*, Math. Annalen, Bd. 105, S. 620–627.

Notation. If a is an element of R and ψ is an automorphism from M, then $\psi(a)$ denotes the image of a under ψ.

II. On the Kernel of a I Ring

THEOREM 1. *Let R be a I ring (i.e. a ring where the chain conditions on right ideals are fulfilled) and let M be a set of automorphisms of R. Then each potent right ideal $\bar{A}$ of the kernel K of R (with respect to M) contains an idempotent element.*

PROOF. According to I, 5 the kernel K possesses a radical $\bar{N}$. If $K = \bar{N}$, then the theorem is obviously true. If $K \neq \bar{N}$, then let a denote an element of the potent right ideal $\bar{A}$ of K such that a does not belong to $\bar{N}$. Then the right ideal aK of K is potent and $aK \subseteq \bar{A}$. Further, aK is not a nilring, since, according to I, 5, each nilring which is a subring of a I-ring is nilpotent. There exists, therefore, an element b in K such that $c = ab$ is a potent element. For each integral λ we then have $c^\lambda \neq 0$, and therefore $c^\lambda R \neq 0$. Since $c^\lambda R \supseteq c^{\lambda+1}R \supseteq c^{\lambda+2}R \supseteq \cdots$ and since R is a I-ring, there exists an integer n such that $c^\nu R = c^\mu R$ if $\nu, \mu \geqq n$. Putting $d = c^{n+1}$ and $A^* = dR$ we have $d \in A^*$ (since $c^n c \in c^n R = A^*$) and $A^* = dA^*$. Applying the last statement made in I, 2 we deduce the existence of an idempotent element e such that $d = de$, $e \in A^*$. If ψ is an arbitrary automorphism belonging to M, then $\psi(d) = \psi(d)\psi(e)$, or (since $\psi(d) = d$ in virtue of $d \in K$) $d = d\psi(e)$; by subtraction we obtain $d[e - \psi(e)] = 0$. The right ideal A^* being normal with respect to M (since $\psi(dR) = \psi(d)\psi(R) = dR$ for each ψ belonging to M) it follows that $\psi(e) \in A^*$ and hence $e - \psi(e) \in A^*$. Applying the last statement of I, 2 we obtain $e - \psi(e) = 0$ or $e = \psi(e)$ for each ψ which belongs to M, i.e. the element e lies in K. From $A^* = dA^*$ and $e \in A^*$ follows the existence of an element $\bar{d}$ in A^* such that $e = d\bar{d}$. If ψ denotes an arbitrary automorphism of R belonging to M, we find in virtue of $\psi(e) = e$, $\psi(d) = d$ that $d[\bar{d} - \psi(\bar{d})] = 0$ and hence (by the last statement of I, 2) $\bar{d} = \psi(\bar{d})$, i.e. $\bar{d} \in K$. Consequently $e \in dK$, and (since $dK \subseteq \bar{A}$) $e \in \bar{A}$, q.e.d.

Applying I, 6 we obtain using the result of the above theorem, the following:

THEOREM 2. *Let R be a I-ring and M a set of automorphisms of R. Then the kernel K of R (with respect to M) is a II-ring (see I, 1).*

III. On the Kernel of a Nilpotent I-Ring

LEMMA 1. *If N is a nilpotent I-ring whose exponent is m (i.e. $N^m \neq 0$, $N^{m+\nu} = 0$ for $\nu \geqq 1$) then also N^λ, $m > \lambda \geqq 1$ is a I-ring.*

We prove the lemma by induction. We first show that N^m is a I-ring. If namely A_m is a right ideal in N^m, then A_m is identical with the right ideal $\bar{A}_m = (A_m, A_mN)$ of N since $A_mN = 0$ in virtue of $A_mN \subseteq N^mN = 0$. Hence, N being a I-ring, also N^m is a I-ring. We assume, that it is already proved that $N^{m-\lambda}$, $m - 1 > \lambda \geqq 1$ is a I-ring, and consider the quotient-ring $N^{m-\lambda-1}/N^{m-\lambda}$ (the ring $N^{m-\lambda}$ is an ideal in N). If $A_{m-\lambda-1}$ is a right ideal in the ring $N^{m-\lambda-1}$, then $\bar{A}_{m-\lambda-1} = (A_{m-\lambda-1}, A_{m-\lambda-1}N)$ is a right ideal in N, and we obtain

$\bar{A}_{m-\lambda-1}/N^{m-\lambda} = (A_{m-\lambda-1}/N^{m-\lambda}, A_{m-\lambda-1}N/N^{m-\lambda}) = A_{m-\lambda-1}/N^{m-\lambda}$ since $A_{m-\lambda-1}N \subseteq N^{m-\lambda}$ and hence $A_{m-\lambda-1}N/N^{m-\lambda} = 0$. Each right ideal of $N^{m-\lambda-1}/N^{m-\lambda}$ is, therefore, a quotient-right ideal of a right ideal of N with respect to $N^{m-\lambda}$, which implies that the quotient-ring $N^{m-\lambda-1}/N^{m-\lambda}$ is a I-ring. But since $N^{m-\lambda}$ and $N^{m-\lambda-1}/N^{m-\lambda}$ are both I-rings it follows that also $N^{m-\lambda-1}$ is a I-ring, which completes the proof of the lemma.

LEMMA 2. *If N is a nilpotent I-ring, then N^λ is a normal subset (ideal) of N with respect to each set of automorphisms of N.*

The proof follows easily from the properties of an automorphism.

LEMMA 3. *If N is a nilpotent I-ring, then the Kernel K_λ of N^λ (with respect to a given set of automorphisms of N) is an ideal in the Kernel K of N.*

Since, namely, $N^\lambda \subseteq N$, we have $K_\lambda \subseteq K$; further $(K_\lambda K, KK_\lambda) \subseteq N^\lambda$; on the other hand $(K_\lambda K, KK_\lambda) \subseteq K$; hence K_λ is an ideal in K.

LEMMA 4. *The kernel K of a nilpotent I-ring R whose exponent is* 1, *is a nilpotent I-ring.*

The proof follows from the fact that each right ideal of an arbitrary subring of such a ring R is also a right ideal of R.

THEOREM 3. *If N is a nilpotent I-ring and M a set of automorphisms of N, then also the Kernel K of N (with respect to M) is a I-ring.*

PROOF. We prove the theorem by induction: If N has the exponent 1, then the theorem is true according to lemma 4. We now assume that the theorem is true for all the nilpotent I-rings whose exponent is smaller than that of N. We consider the nilpotent ring N/N^2 which is also a I-ring. Further, also the ring K/N^2 is a I-ring since K/N^2 is a subset of the I-ring N/N^2 whose exponent is 1 (see lemma 4). Hence, there exists a finite set of elements $k_1, \cdots, k_m$ in K such that each element k of K can be written in the form $k = \sum_{i=1}^m n_i k_i + c$ where the n_i are integers and $c \in N^2$. Since $k \in K$ and $n_i k_i \in K$ it follows that $c \in K$. From $c \in K$ and $c \in N^2$ we obtain $c \in K_2$, where K_2 is the kernel of N^2. According to lemma 3 we know that K_2 is an ideal in K. If k_i^* is the element of K/K_2 which corresponds to k_i, then the k_i^* are different from each other, since $K/K_2 \sim K/N^2$ (i.e.: K/N^2 is homomorphic with K/K_2). Since each k which lies in K has the above mentioned form $k = \sum_{i=1}^m n_i k_i + c$, it follows that the rings K/K_2 and K/N^2 are even isomorphic (in short: $K/K_2 \simeq K/N^2$). Hence (since, as mentioned above K/N^2 is a I-ring) K/K_2 is a I-ring. Since N^2 is a I-ring (lemma 1) whose exponent is smaller than that of N, we may assume according to our inductional proposition that K_2 is a I-ring. But together with K/K_2 and K_2 also K is a I-ring, q.e.d.

IV. THE SET M OF THE AUTOMORPHISMS FORMS A FINITE GROUP

THEOREM 4. *If R is a I-ring and n is the order of a finite group $M = \psi_1, \cdots, \psi_m$ of automorphisms of R, and if $na \neq 0$ for each element $a \neq 0$ of R, then the kernel K' of an arbitrary normal right ideal A of R is potent if and only if A is potent.*

PROOF. If A is nilpotent, then K' is obviously nilpotent. Let now A be potent. Let $\bar{A}$ be a normal-primitive right ideal of R which lies in A. Such

a right ideal exists, since the class of the normal right ideals of R which lie in A is not empty (A being one of them) and since R is a I-ring. Let d be a principal idempotent element of $\bar{A}$. We consider the elements $d_i = \psi_i(d)$, $i = 1, \cdots m$ where the ψ_i are the elements of the group M. From the properties of an isomorphism it follows that also the d_i are principal idempotent elements of $\bar{A}$ since $\bar{A}$ is normal with respect to M. The element $a = \sum_{i=1}^{m} d_i$ which lies in $\bar{A}$ remains invariant under each automorphism from M, i.e. it lies in the kernel K of R, and hence also in the kernel K' of $\bar{A}$. On the other hand, this element is potent (see I, 4). Hence also K' is potent, q.e.d.

THEOREM 5. *If the conditions of the foregoing theorem are fulfilled, then each normal-primitive right ideal A of R possesses a left hand unit, which belongs to the kernel of R.*

PROOF. First note that the kernel of a right ideal is a right ideal in the kernel of the ring. According to theorem 4 this right ideal is potent and possesses in virtue of theorem 1 an idempotent element e. Since $e \varepsilon A$ we have $eA \subseteq A$ and since eA is potent and normal we obtain $eA = A$ (since A is normal-primitive). Hence A contains the left hand unit e which lies in the kernel of R.

We now obtain the following correspondence between the *normal-primitive* right ideals of R and the *primitive* right ideals of the kernel of R.

THEOREM 6. *If the conditions of theorem 4 are fulfilled, then: α) The kernel K' of a normal-primitive right ideal A of R is a primitive right ideal of the kernel K of R. β) The right ideal $(A', A'R)$ of R which is derived from a primitive right-ideal A' of K is a normal-primitive right ideal of R.*

PROOF. α) The kernel K' of A is a potent right ideal of the kernel K of R (see theorem 4), and since K is a II-ring (theorem 2), it follows that K' contains a primitive right ideal A'. Let e' be a left hand unit of A', then $A' = e'K' \subseteq K'$; suppose $e'K' \subset K'$, i.e. e' were not a left hand unit of K', then let e be a left hand unit of A which lies in K (theorem 5); then $e \varepsilon K'$. If we put $e^* = e - e'e$ then $e^* \neq 0$ in virtue of $e'e \neq e$ (otherwise e' would be a left hand unit of K') and $e^* = e^{*2}$, $e^*e' = e'e^*$; we obtain $A = e^*A + e'A$, where e^*A, $e'A$ are normal potent right ideals, which contradicts the assumption that A is normal-primitive. Hence $A' = K'$ i.e. K' is a primitive right ideal of K. β) The right ideal $A = (A', A'R)$ of R, where A' is primitive in K has the form $A = e'R$, where e' is a left hand unit of A' (see theorem 2 and I, 2). Let A^* be a normal-primitive right ideal of R which lies in A. Let e^* be a left hand unit of A^* which is contained in K (theorem 5). Suppose $A^* \subset A$, then we put $e'' = e' - e^*e$). The element e'' lies in K and it follows as above that $e''^2 = e'' \neq 0$ and $e''e^* = e^*e'' = 0$; hence $A' = e^*A' + e''A'$, which contradicts the assumption that A' is primitive. Hence $A^* = A$, i.e. A is normal-primitive.

THEOREM 7. *If the conditions of theorem 4 are fulfilled, then the radical of the kernel K of R is a subset of the radical of R.*

PROOF. Let c be an element of the radical of K. If c were not an element of the radical of R, then the normal right ideal cR of R would be potent and would possess an idempotent element d which lies in K. We put $d = cb$, then

$\sum_{i=1}^{m} \psi_i(d) = \sum_{i=1}^{m} \psi_i(cb)$ where the ψ_i are the elements of the given group of automorphisms of R; since $\sum_{i=1}^{m} \psi_i(d) = nd$ and $\psi_i(cb) = \psi_i(c)\psi_i(b) = c\psi_i(b)$ we obtain $nd = c \sum_{i=1}^{m} \psi_i(b) = ca$ where $a = \sum_{i=1}^{m} \psi_i(b)$. Since $a \in K$ it follows that ca lies in the radical of K, hence, for a certain integer λ we have the relation $(ca)^\lambda = 0$. But this implies $(nd)^\lambda = 0$ or $n^\lambda d = 0$ which contradicts one of the assumptions of our theorem (see theorem 4). This shows the truth of our theorem.

THEOREM 8. *If the ring R and its radical are both I-rings, then under the conditions of theorem 4 also the kernel of R and its radical are both I-rings.*

PROOF. This theorem follows from theorems 2, 3 and 7.

As an immediate consequence of theorem 7 follows

THEOREM 9. *If R is a semi simple ring, then under the conditions of theorem 4 the kernel of R is also a semi simple ring.*

PROOF. If the radical of K were not zero, then also the radical of R which contains the radical of K (theorem 7) would differ from zero, which contradicts the assumption that R is semi simple.

The results of the present paragraph were found under the assumption that the set M of the automorphisms of R forms a finite group and that $na = 0$ implies $a = 0$ for each element a which lies in R (n is the order of the group M). The following examples show the necessity of these conditions.

Example 1. Let R be the ring of all the two-rowed quadratic matrices in the field of the rational numbers. We transform R by a matrix $\begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix}$ where g_λ is a positive or a negative integer or zero. This transformation defines an automorphism of R. The set M of all the matrices of the form $\begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix}$ is an infinite group. The set A of all the matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ defines a normal right-ideal of R (with respect to M), since $\begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix}^{-1} = A$. If $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ belongs to the kernel K' of A, then $\begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix}$ which implies for $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ the necessary condition $a = 0$, which is also sufficient in order that $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in K'$; i.e. the kernel K' of A is identical with the set of all the matrices $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ and is therefore nilpotent, while A is potent. Hence, theorem 4 does not hold. If now K is the kernel of R with respect to M, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K$ if $\begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & g_\lambda \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ holds for each integer g_λ, which implies $c = 0$, $a = d$. K is identical with the set of all the matrices of the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$;

the radical of K is not zero, since the set of all the matrices of the form $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ is a nilpotent right ideal of K. Hence, the theorems 7 and 9 do not hold.

Example 2. Let R be the ring of all the quadratic two-rowed matrices in a field of characteristic 2. If we transform R with the two matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ we obtain a group of automorphisms of R whose order is 2, since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1+1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ on account of $1 + 1 = 0$. The potent right ideal A of all the matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ is as in example 1 normal with respect to M. If K' is the kernel of A with respect to M, then we find as in example 1 that K' consists of all the matrices of the form $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, and is therefore nilpotent. Hence, the theorem 4 does not hold. If K denotes the kernel of R under M, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lies in K if and only if $c = 0$, $a = d$. Hence K consists of all the matrices of the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ and contains, as in example 1 a radical which is not zero. Hence, theorems 7 and 9 do not hold.

V. The Semi Simplicity of a Group Algebra

As an application of the foregoing paragraph we shall now derive a new proof for the theorem which states that the algebra of a finite group over a field whose characteristic does not divide the order of the group, is a semi simple algebra. Let R be the algebra of the finite group $\Gamma = g_1, \cdots, g_n$ over the field F. Let $\bar{\Gamma}$ be the automorphism-group of R which is induced by transforming the ring R with the elements g_i. Each ideal A of R is transformed into itself (in other words: A is normal with respect to $\bar{\Gamma}$). The primary ideals (i.e. potent ideals which do not contain other potent ideals besides themselves) and the normal primitive right and left ideals are identical sets. Let A be a primary ideal. The kernel of A is then a potent ring (theorem 4) and possesses an idempotent element e. Since $eA \subseteq A$ and eA is normal, while A is normal-primitive, we have $eA = A$. Similarly $Ae = A$; hence e is the unit of A. This implies (according to known facts on algebras) that R is a direct sum of primary ideals with units. We have to prove now that each primary ideal is simple. Without losing the generality we may assume that F is an algebraically closed field, then $A = B \times C$ where B is a total matric algebra over F, and C is an algebra whose quotient algebra with respect to its radical N is isomorphic with F. The ideal A possesses a radical which is different from zero if and only if N is different from zero. Suppose $N^{\lambda+1} = 0$, $N^\lambda \neq 0$, $\lambda > 1$, then each element q of N^λ lies in the centre of C, since, F being algebraically closed, each element c of C has the form $c = p + t$, where $p \,\varepsilon\, F$ and $t \,\varepsilon\, N$; from

$qp = pq$, $qt = tq$ (in virtue of qt, $tq \varepsilon N^\lambda = 0$) it follows that $qc = cq$, hence q lies in the centre of C. Since $A = B \times C$, it follows that N^λ belongs also to the centre of A. If $\bar{g}_i$ is the component of g_i in A (i.e. $\bar{g}_i = eg_i$ where e is the unit of A) and if we consider an arbitrary simple algebra A^* which contains A (such algebras over F exist), then the transformations of A^* with the elements $\bar{g}_i$ define an automorphism-group Γ^* of A^* (even of A) under which each element of N^λ remains invariant, hence N^λ belongs to the kernel K^* of A^*. The algebra K^* is semi-simple (theorem 9), and since $k^*\bar{g}_i = \bar{g}_i k^*$ for each $k^* \varepsilon K^*$, hence $k^*a^* = a^*k^*$ for each a^* which lies in A, we have in particular $N^\lambda K^* = K^* N^\lambda$ which implies $(N^\lambda K^*)^2 = N^{2\lambda} K^* = 0$. On the other hand, $N^\lambda K^*$ is an ideal in K^*, and since K^* is semi simple, each power of $N^\lambda K^*$ must be different from zero. This contradiction implies $N = 0$, i.e. A is simple, and hence R semi simple, q.e.d.

New Haven, Conn.

Egleston

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

SECOND SERIES, VOL. 36, NO. 1

JANUARY, 1935

PUBLISHED QUARTERLY
AT
MOUNT ROYAL AND GUILFORD AVENUES
BALTIMORE, MD.
BY THE
PRINCETON UNIVERSITY PRESS
PRINCETON, N. J.

ANNALS OF MATHEMATICS

Subscription price, $5, a volume (four numbers) in advance. Single copies $1.50. An arrangement has been made with the Mathematical Association of America in accordance with which an individual member of the Association may subscribe to the Annals of Mathematics at one-half the regular price. Subscriptions, orders for back numbers and changes of address should be sent to Mount Royal and Guilford Avenues, Baltimore, Md., or to the Princeton University Press, Princeton, New Jersey.

Manuscripts and all editorial correspondence should be addressed to The Annals of Mathematics, Fine Hall, Princeton, New Jersey. Manuscripts should be typewritten, with the exception of formulae, and must be in final form with all references filled in.

Authors receive gratis 100 reprints of each article, postage prepaid.

Entered as second class matter at the Post Office at Baltimore, Maryland, under the Act of March 3, 1879.

Made in United States of America

TABLE OF CONTENTS

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

SECOND SERIES, VOL. 36, NO. 2

APRIL, 1935

PUBLISHED QUARTERLY
AT
MOUNT ROYAL AND GUILFORD AVENUES
BALTIMORE, MD.
BY THE
PRINCETON UNIVERSITY PRESS
PRINCETON, N. J.

ANNALS OF MATHEMATICS

Subscription price, $5 a volume (four numbers) in advance. Single copies $1.50. An arrangement has been made with the Mathematical Association of America in accordance with which an individual member of the Association may subscribe to the Annals of Mathematics at one-half the regular price. Subscriptions, orders for back numbers and changes of address should be sent to Mount Royal and Guilford Avenues, Baltimore, Md., or to the Princeton University Press, Princeton, New Jersey.

Manuscripts and all editorial correspondence should be addressed to The Annals of Mathematics, Fine Hall, Princeton, New Jersey. Manuscripts should be typewritten, with the exception of formulae, and must be in final form with all references filled in.

Authors receive gratis 100 reprints of each article, postage prepaid.

Entered as second class matter at the Post Office at Baltimore, Maryland, under the Act of March 3, 1879.

Made in United States of America

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

SECOND SERIES, VOL. 36, NO. 3

JULY, 1935

PUBLISHED QUARTERLY
AT
MOUNT ROYAL AND GUILFORD AVENUES
BALTIMORE, MD.
BY THE
PRINCETON UNIVERSITY PRESS
PRINCETON, N. J.

ANNALS OF MATHEMATICS

Subscription price, \$5 a volume (four numbers) in advance. Single copies \$1.50. An arrangement has been made with the Mathematical Association of America in accordance with which an individual member of the Association may subscribe to the Annals of Mathematics at one-half the regular price. Subscriptions, orders for back numbers and changes of address should be sent to Mount Royal and Guilford Avenues, Baltimore, Md., or to the Princeton University Press, Princeton, New Jersey.

Manuscripts and all editorial correspondence should be addressed to The Annals of Mathematics, Fine Hall, Princeton, New Jersey. Manuscripts should be typewritten, with the exception of formulae, and must be in final form with all references filled in.

Authors receive gratis 100 reprints of each article, postage prepaid.

Entered as second-class matter at the Post Office at Baltimore, Maryland, under the Act of March 3, 1879.

Made in United States of America

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

SECOND SERIES, VOL. 36, NO. 4

OCTOBER, 1935

PUBLISHED QUARTERLY
AT
MOUNT ROYAL AND GUILFORD AVENUES
BALTIMORE, MD.
BY THE
PRINCETON UNIVERSITY PRESS
PRINCETON, N. J.

ANNALS OF MATHEMATICS

Subscription price, $5 a volume (four numbers) in advance. Single copies $1.50. An arrangement has been made with the Mathematical Association of America in accordance with which an individual member of the Association may subscribe to the Annals of Mathematics at one-half the regular price. Subscriptions, orders for back numbers and changes of address should be sent to Mount Royal and Guilford Avenues, Baltimore, Md., or to the Princeton University Press, Princeton, New Jersey.

Manuscripts and all editorial correspondence should be addressed to The Annals of Mathematics, Fine Hall, Princeton, New Jersey. Manuscripts should be typewritten, with the exception of formulae, and must be in final form with all references filled in.

Authors receive gratis 100 reprints of each article, postage prepaid.

Entered as second-class matter at the Post Office at Baltimore, Maryland, under the Act of March 3, 1879.

Made in United States of America